PATENT ABSTRACTS OF JAPAN

(11)Publication number : 10-133955
(43)Date of publication of application : 22.05.1998

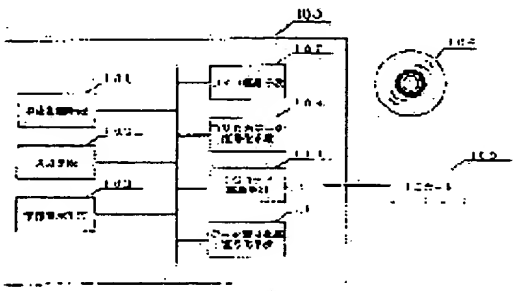
(51)Int.Cl. G06F 12/14
G06F 12/00
G09C 1/00
H04L 9/08
H04L 9/14

(21)Application number : 08-286345
(22)Date of filing : 29.10.1996

(71)Applicant : MATSUSHITA ELECTRIC IND CO LTD
(72)Inventor : URANAKA SACHIKO
KIYONO MASAKI

(54) PORTABLE MEDIUM DRIVING DEVICE, ITS METHOD, COOPERATIVE DEVICE OF PORTABLE MEDIUM AND NETWORK, AND ITS METHOD

(57)Abstract:
PROBLEM TO BE SOLVED: To eliminate the illegal use of a portable medium at the time of using the portable medium individually or in cooperation with a network.
SOLUTION: Data ciphered by a data ciphering key D is recorded in the portable medium 106 and a ciphered data ciphering key ciphered by using a user's open key PU in an open key ciphering system is recorded at a part different from the original storing area of the medium 106. A portable medium reproducing device is provided with a means capable of obtaining the secret key PS of the user to decode a data ciphering key D by a data ciphering key decoding means 111 through the use of this key PS and to restore data within the medium 106 by an in-DVD data restoring means 108 through the use of this key D to display. In addition, by constituting to obtain a ciphered data ciphering key through the network, the using quantity or the using effective time limit of the medium 106 are managed, charging is executed and using is restricted.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平10－133955

(43)公開日　平成10年(1998)５月22日

(51)Int.Cl.[6]		識別記号	Ｆ１		
Ｇ０６Ｆ	12/14	３２０	Ｇ０６Ｆ	12/14	３２０Ｄ
	12/00	５３７		12/00	５３７Ｈ
Ｇ０９Ｃ	1/00	６６０	Ｇ０９Ｃ	1/00	６６０Ｄ
Ｈ０４Ｌ	9/08		Ｈ０４Ｌ	9/00	６０１Ａ
	9/14				６０１Ｅ

審査請求　未請求　請求項の数24　ＯＬ　（全 54 頁）　最終頁に続く

(21)出願番号　特願平8－286345

(22)出願日　平成８年(1996)10月29日

(71)出願人　000005821
松下電器産業株式会社
大阪府門真市大字門真1006番地

(72)発明者　浦中　祥子
大阪府門真市大字門真1006番地　松下電器産業株式会社内

(72)発明者　清野　正樹
大阪府門真市大字門真1006番地　松下電器産業株式会社内

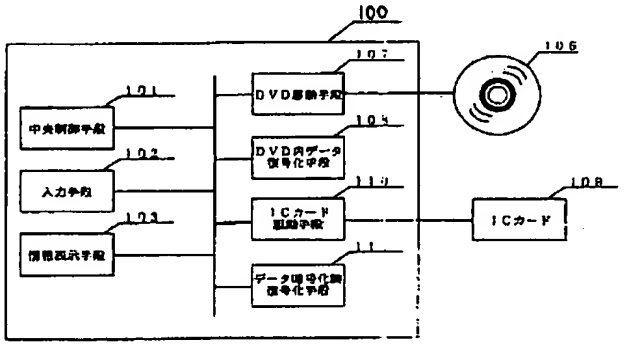
(74)代理人　弁理士　滝本　智之　（外１名）

(54)【発明の名称】　可搬型メディア駆動装置とその方法、及び可搬型メディアとネットワークの連携装置とその方法

(57)【要約】

【課題】　可搬型メディアを単独で、あるいはネットワークと連携して用いる場合に、その不正使用を排除することを目的とする。

【解決手段】　可搬型メディア１０６にはデータ暗号化鍵Ｄで暗号化されたデータを記録しておき、可搬型メディア１０６の本来の記憶領域とは異なる部分に、公開鍵暗号方式における利用者の公開鍵ＰＵを用いて暗号化された暗号化データ暗号化鍵を記録しておく。可搬型メディア再生装置には利用者の秘密鍵ＰＳを取得できる手段を備えておき、この利用者秘密鍵ＰＳを用いてデータ暗号化鍵復号化手段１１１によりデータ暗号化鍵Ｄを復号化し、さらにこのデータ暗号化鍵Ｄを用いてＤＶＤ内データ復号化手段１０８により可搬型メディア１０６内のデータを復元して表示する。また、ネットワークを通じて、暗号化データ暗号化鍵を取得する構成にすることにより、可搬型メディア１０６の使用量、あるいは使用有効期限を管理し、課金を施したり、使用を制限する。



【特許請求の範囲】

【請求項１】　それぞれに固有なメディア活用情報と、データ暗号化鍵によって暗号化された暗号化データとを記録し、前記メディア活用情報としては、データ暗号化鍵を、利用者ごとの秘密情報で復号可能な形式で暗号化した、暗号化データ暗号化鍵を少なくとも含んだ可搬型メディアから、

前記暗号化データを解読する装置であり、その構成としては、前記可搬型メディアを駆動する可搬型メディア駆動手段と、利用者ごとの秘密情報を取得する秘密情報取得手段と、前記可搬型メディアに記録されている暗号化データを前記データ暗号化鍵を用いて復号化しデータを生成する第１のデータ復号化手段と、前記秘密情報取得手段で取得した利用者ごとの秘密情報を用いてメディア活用情報に含まれている前記暗号化データ暗号化鍵を復号化してデータ暗号化鍵を生成する第２のデータ復号化手段とを備え、

利用者ごとの秘密情報と暗号化データ暗号化鍵とを用いて、可搬型メディア内の暗号化データを復号化してデータを生成することを特徴とする可搬型メディア駆動装置。

【請求項２】　それぞれに固有なメディア活用情報と、データ暗号化鍵によって暗号化された暗号化データとを記録し、前記メディア活用情報としては、データ暗号化鍵を、利用者ごとの秘密情報で復号可能な形式で暗号化した、暗号化データ暗号化鍵を少なくとも含んだ可搬型メディアから、前記暗号化データ暗号化鍵を得るステップと、

前記ステップと同時にあるいはその前後に利用者ごとの秘密情報を得るステップと、

前記得られた利用者ごとの秘密情報を用いて、前記暗号化データ暗号化鍵を復号化してデータ暗号化鍵を生成するステップと、

前記データ暗号化鍵を用いて、前記可搬型メディアに記録されている暗号化データを復号化してデータを生成するステップとからなる可搬型メディア駆動方法。

【請求項３】　それぞれに固有なメディア活用情報と、データ暗号化鍵によって暗号化された暗号化データとを記録した可搬型メディアと、前記暗号化データを解読する第１の電子計算機と、前記解読に必要な情報を前記第１の電子計算機に提供する第２の電子計算機と、前記第１と第２の電子計算機を繋ぐネットワークとから構成され、

前記メディア活用情報としては、前記可搬型メディアに記録されているデータの種類に対応する情報であるタイトル情報と、前記可搬型メディアと他とを区別する情報である前記タイトル情報ごとの発行番号情報とを少なくとも含み、

前記第１の電子計算機は、前記可搬型メディアを駆動する可搬型メディア駆動手段と、利用者ごとの秘密情報を格納する第１の秘密情報格納手段と、前記可搬型メディアに記録されている暗号化データをデータ暗号化鍵を用いて復号化しデータを生成する第１のデータ復号化手段と、前記ネットワークに対する入出力を行なう第１の情報送受信手段と、前記利用者ごとの秘密情報を用いて復号化する第２のデータ復号化手段とを備え、

前記第２の電子計算機は、前記可搬型メディアに記録されている暗号化データの暗号化に用いたデータ暗号化鍵を、タイトル情報ごとに管理する可搬型メディア情報管理手段と、前記第１の秘密情報格納手段に格納されている利用者ごとの秘密情報と一対の公開情報を、発行番号情報ごとに管理する利用者情報管理手段と、前記公開情報を用いてデータ暗号化鍵を暗号化して暗号化データ暗号化鍵を生成するデータ暗号化手段と、前記ネットワークに対する入出力を行なう第２の情報送受信手段とを備え、

前記公開情報と前記秘密情報とは、公開情報を用いてデータを変換すると、秘密情報を用いてしか復元できない関係にあり、

前記データ暗号化手段によって生成された暗号化データ暗号化鍵を第２の電子計算機から第１の電子計算機に送信した後、前記第２のデータ復号化手段が前記暗号化データ暗号化鍵を復号化してデータ暗号化鍵を生成することを特徴とする可搬型メディアとネットワークの連携装置。

【請求項４】　第２の電子計算機が、任意のデータに対して、その時限りの疑似変化を与えることのできる疑似変化情報を生成する疑似変化情報生成手段を更に備え、データ暗号化手段が、前記疑似変化情報と公開情報とを用いて暗号化データ暗号化鍵を生成することを特徴とする請求項３に記載の可搬型メディアとネットワークの連携装置。

【請求項５】　第１の電子計算機において、それぞれに固有なメディア活用情報と、データ暗号化鍵によって暗号化された暗号化データとを記録し、前記メディア活用情報としては、前記可搬型メディアに記録されているデータの種類に対応する情報であるタイトル情報と、前記可搬型メディアと他とを区別する情報である前記タイトル情報ごとの発行番号情報とを少なくとも含んだ可搬型メディアから、前記タイトル情報と前記発行番号情報とを得るステップと、前記タイトル情報と前記発行番号情報とをネットワークを経由して第２の電子計算機に送信するステップと、

前記第２の電子計算機において、前記タイトル情報と前記発行番号情報とを受信するステップと、前記タイトル情報から前記データ暗号化鍵を得るステップと、前記タイトル情報と前記発行番号情報とから、利用者ごとの秘密情報と一対の公開情報を得るステップと、任意のデータに対して、その時限りの疑似変化を与える疑似変化情報を生成するステップと、前記疑似変化情報と前記公開

情報とを用いて前記データ暗号化鍵を暗号化して暗号化データ暗号化鍵を生成するステップと、前記暗号化データ暗号化鍵を前記第１の電子計算機にネットワークを経由して送信するステップと、
前記第１の電子計算機において、前記暗号化データ暗号化鍵を受信するステップと、前記公開情報により変換されたデータに対して唯一復元可能な前記利用者ごとの秘密情報を得るステップと、前記秘密情報を用いて前記暗号化データ暗号化鍵を復号化してデータ暗号化鍵を生成するステップと、前記データ暗号化鍵を用いて可搬型メディアに記録されている暗号化データを復号化してデータを生成するステップとからなる可搬型メディアとネットワークの連携方法。

【請求項６】　それぞれに固有なメディア活用情報を記録した可搬型メディアと、第１の電子計算機と、第２の電子計算機と、前記第１と第２の電子計算機の間を結ぶネットワークとから構成され、
前記第１の電子計算機は、前記可搬型メディアを駆動する可搬型メディア駆動手段と、データを暗号化するデータ暗号化手段と、前記ネットワークに対する入出力を行なう第１の情報送受信手段とを備え、
前記第２の電子計算機は、それぞれに固有な秘密情報を格納する第２の秘密情報格納手段と、任意のデータに対して、その時限りの疑似変化を与える疑似変化情報を生成する疑似変化情報発生手段と、前記疑似変化情報など、情報を記憶する情報記憶手段と、データを復号化するデータ復号化手段と、前記ネットワークに対する入出力を行なう第２の情報送受信手段とを備え、
前記メディア活用情報としては、前記第２の秘密情報格納手段に格納された秘密情報と一対の公開情報が少なくとも含まれており、
前記公開情報と前記秘密情報とは、公開情報を用いてデータを変換すると、秘密情報を用いてしか復元できない関係にあり、
前記データ暗号化手段が、前記第２の電子計算機より送信される疑似変化情報と前記メディア活用情報に含まれる公開情報とを用いて、データを暗号化し、暗号化データを生成し、
前記データ復号化手段が、前記情報記憶手段により記憶しておいた疑似変化情報と前記第２の秘密情報格納手段に格納されている秘密情報とを用いて前記データ暗号化手段によって生成された暗号化データの復号化を行うことを特徴とする可搬型メディアとネットワークの連携装置。

【請求項７】　第２の電子計算機において、第１の電子計算機の要求を受けて、任意のデータに対し、その時限りの疑似変化を与える疑似変化情報を生成するステップと、前記疑似変化情報を記憶し、前記第１の電子計算機にネットワークを経由して送信するステップと、
前記第１の電子計算機において、前記送信された疑似変化情報を受信するステップと、可搬型メディアに記録されているメディア活用情報が含んでいる公開情報を得るステップと、前記疑似変化情報と前記公開情報とを用いてデータを暗号化して暗号化データを生成するステップと、前記暗号化データを前記第２の電子計算機にネットワークを経由して送信するステップと、
前記第２の電子計算機において、前記暗号化データを受信するステップと、前記公開情報により変換されたデータに対して唯一復元可能な、秘密情報を得るステップと、前記記憶しておいた疑似変化情報と秘密情報とを用いて暗号化データを復号化してデータを生成するステップとからなる可搬型メディアとネットワークの連携方法。

【請求項８】　それぞれに固有なメディア活用情報を記録した可搬型メディアと、第１の電子計算機と、第２の電子計算機と、前記第１と第２の電子計算機の間を結ぶネットワークとから構成され、
前記第１の電子計算機は、前記可搬型メディアを駆動する可搬型メディア駆動手段と、前記ネットワークに対する入出力を行なう第１の情報送受信手段とを備え、
前記第２の電子計算機は、前記可搬型メディアの使用量を管理する可搬型メディア使用量管理手段と、前記ネットワークに対する入出力を行なう第２の情報送受信手段とを備え、
前記メディア活用情報としては、前記可搬型メディア内のデータの種類に対応する情報としてのタイトル情報と、前記可搬型メディアと他とを区別する情報としての前記タイトル情報ごとの発行番号情報とが少なくとも含まれており、
前記可搬型メディア使用量管理手段が、前記第１の電子計算機から送信される前記タイトル情報と前記発行番号情報とを用いて可搬型メディアを特定して該メディアの使用量を管理することを特徴とする可搬型メディアとネットワークの連携装置。

【請求項９】　第１の電子計算機において、可搬型メディアに記録されているメディア活用情報に含まれているタイトル情報と発行番号情報とを得るステップと、前記タイトル情報と前記発行番号情報とを第２の電子計算機にネットワークを経由して送信するステップと、
前記第２の電子計算機において、前記使用量と前記タイトル情報と前記発行番号情報とを受信するステップと、前記タイトル情報の前記発行番号情報に対して既に使用量が記録されている場合には、前記使用量に対して、新たなる使用量を加算するステップと、前記タイトル情報の前記発行番号情報に対して使用量が記録されていない場合には、前記タイトル情報の前記発行番号情報に対応するエントリを新たに作成し、該メディアの使用量として、前記使用量を記録するステップとからなる可搬型メディアとネットワークの連携方法。

【請求項１０】　メディア使用量管理手段において、タ

イトル情報と発行番号情報に加え、該メディア内のデータ名などをも用いてデータごとの使用量を階層的に管理することを特徴とする、請求項８に記載の可搬型メディアとネットワークの連携装置。

【請求項１１】　メディア使用量管理手段が、タイトル情報と発行番号情報ごとの使用量に加え、該可搬型メディアの最大使用量を管理し、使用量が最大使用量を超えているかどうかを判断することを特徴とする請求項８に記載の可搬型メディアとネットワークの連携装置。

【請求項１２】　メディア活用情報の一部として、タイトル情報と発行番号情報とに加え、該可搬型メディアの最大使用量を更に設け、

前記タイトル情報の前記発行番号情報のデータ使用量がメディア使用量管理手段に記録されていない場合には、メディア活用情報に記録されている最大使用量をメディア使用量管理手段における前記タイトル情報の前記発行番号情報の最大使用量として記録することを特徴とする請求項１１に記載の可搬型メディアとネットワークの連携装置。

【請求項１３】　可搬型メディアが、メディア活用情報に加え、データ暗号化鍵によって暗号化された暗号化データを更に記録し、

第１の電子計算機が、利用者ごとの秘密情報を格納する第１の秘密情報格納手段と、前記暗号化データをデータ暗号化鍵を用いて復号化しデータを生成する第１のデータ復号化手段と、前記利用者ごとの秘密情報を用いて復号化する第２のデータ復号化手段とを更に備え、

第２の電子計算機が、前記可搬型メディアに記録されている暗号化データの暗号化に用いたデータ暗号化鍵を、タイトル情報ごとに管理する可搬型メディア情報管理手段と、前記公開情報を用いてデータ暗号化鍵を暗号化して暗号化データ暗号化鍵を生成するデータ暗号化手段とを更に備え、

可搬型メディア使用量管理手段が、前記可搬型メディアの使用量に加え、前記第１の秘密情報格納手段に格納されている利用者ごとの秘密情報と一対の公開情報も、発行番号情報ごとに管理しており、

前記公開情報と前記秘密情報とは、公開情報を用いてデータを変換すると、秘密情報を用いてしか復元できない関係にあり、

可搬型メディアの使用量が最大使用量を超えていない場合、前記暗号化手段によって生成された暗号化データ暗号化鍵を第１の電子計算機から第２の電子計算機に送信した後、前記第２のデータ復号化手段が前記暗号化データ暗号化鍵を復号化してデータ暗号化鍵を生成することを特徴とする請求項１１又は請求項１２に記載の可搬型メディアとネットワークの連携装置。

【請求項１４】　第１の電子計算機が、データを暗号化するデータ暗号化手段を更に備え、

第２の電子計算機が、それぞれに固有な秘密情報を格納する第２の秘密格納手段と、任意のデータに対して、その時限りの疑似変化を与える疑似変化情報を生成する疑似変化情報生成手段と、前記疑似変化情報などの情報を記憶する情報記憶手段と、データを復号するデータ復号化手段とを更に備え、

可搬型メディアに記録されているメディア活用情報としては、前記第２の秘密情報格納手段に格納された秘密情報と一対の公開情報を更に含み、

前記公開情報と前記秘密情報とは、公開情報を用いてデータを変換すると、秘密情報を用いてしか復元できない関係にあり、

前記データ暗号化手段が、前記第２の電子計算機より送信された疑似変化情報と前記メディア活用情報に含まれる公開情報を用いて、タイトル情報と発行番号情報とを暗号化し、

前記データ復号化手段が、前記情報記憶手段により記憶しておいた疑似変化情報と前記第２の秘密情報格納手段に格納されている秘密情報とを用いて、前記暗号化されたタイトル情報と発行番号情報とを復号化し、

可搬型メディア使用量管理手段が、前記復号化されたタイトル情報と発行番号情報とを用いて、可搬型メディアを特定して該メディアの使用量を管理することを特徴とする請求項８に記載の可搬型メディアとネットワークの連携装置。

【請求項１５】　それぞれに固有なメディア活用情報を記録した可搬型メディアと、前記可搬型メディアを再生する第１の電子計算機と、前記可搬型メディアの使用期限を管理する第２の電子計算機と、前記第１と第２の電子計算機の間を結ぶネットワークとから構成され、

前記メディア活用情報としては、前記可搬型メディア内のデータの種類に対応する情報としてのタイトル情報が少なくとも含まれており、

前記第１の電子計算機は、前記可搬型メディアを駆動する可搬型メディア駆動手段と、前記ネットワークに対する入出力を行なう第１の情報送受信手段とを備え、

前記第２の電子計算機は、前記タイトル情報によって特定される可搬型メディアの使用期限を管理する可搬型メディア使用期限管理手段と、前記特定される可搬型メディアが使用有効期限内であるかどうかを判断する使用有効期限判断手段と、前記ネットワークに対する入出力を行なう第２の情報送受信手段とを備え、

第１の電子計算機において可搬型メディアを使用する際に、タイトル情報を第２の電子計算機に送信し、第２の電子計算機において、各可搬型メディア毎に使用有効期限内であるかどうかを判断することを特徴とする可搬型メディアとネットワークの連携装置。

【請求項１６】　第１の電子計算機において、可搬型メディアに記録されているメディア活用情報に含まれているタイトル情報を得るステップと、前記タイトル情報を第２の電子計算機にネットワークを経由して送信するス

テップと、
前記第２の電子計算機において、前記タイトル情報を受信するステップと、前記タイトル情報に該当するメディアの使用有効期限情報を得るステップと、前記使用有効期限情報に基づき、前記メディアが使用有効期限内であるかどうかを判断するステップとからなる可搬型メディアとネットワークの連携方法。
【請求項１７】　メディア活用情報の一部として、タイトル情報に加え、タイトル情報ごとの発行番号情報も更に含み、
可搬型メディア使用有効期限管理手段は、前記タイトル情報ごとの発行番号情報によって可搬型メディアを特定し、
第１の電子計算機から第２の電子計算機にタイトル情報を送信する際に、発行番号情報も同時に送信し、タイトル情報ごとの発行番号情報によって使用有効期限を管理することを特徴とする請求項１５に記載の可搬型メディアとネットワークの連携装置。
【請求項１８】　メディア使用有効期限管理手段において、タイトル情報に加え、該メディア内のデータ名をも用いてデータごとの使用有効期限を階層的に管理することを特徴とする、請求項１５に記載の可搬型メディアとネットワークの連携装置。
【請求項１９】　それぞれに固有なメディア活用情報を記録した可搬型メディアと、前記可搬型メディアを再生する第１の電子計算機と、前記可搬型メディアの使用期限を管理するする第２の電子計算機と、前記第１と第２の電子計算機の間を結ぶネットワークとから構成され、
前記メディア活用情報としては、該可搬型メディアの有効期限を示す使用有効期限情報が少なくとも含まれており、
前記第１の電子計算機は、前記可搬型メディアを駆動する可搬型メディア駆動手段と、前記ネットワークに対する入出力を行なう第１の情報送受信手段とを備え、
前記第２の電子計算機は、該当する可搬型メディアが使用有効期限内であるかどうかを判断する可搬型メディア使用有効期限判断手段と、前記ネットワークに対する入出力を行なう第２の情報送受信手段とを備え、
第１の電子計算機において可搬型メディアを使用する際に、前記メディア活用情報に含まれる使用有効期限情報を第２の電子計算機に送信し、第２の電子計算機において該可搬型メディアが使用有効期限内かどうかを判断することを特徴とする可搬型メディアとネットワークの連携装置。
【請求項２０】　第１の電子計算機において、可搬型メディアに記録されおり、前記可搬型メディアにそれぞれ固有なメディア活用情報に含まれている前記可搬型メディアの使用有効期限情報を得るステップと、前記使用有効期限情報を第２の電子計算機にネットワークを経由して送信するステップと、
前記第２の電子計算機において、前記使用有効期限情報を受信するステップと、前記使用有効期限情報に基づき、前記可搬型メディアが使用有効期限内であるかどうか判断するステップとからなる可搬型メディアとネットワークの連携方法。
【請求項２１】　メディア活用情報の一部として、可搬型メディア内に記録されている各データごとの使用有効期限情報を階層的に設け、メディア使用有効期限判断手段が、各データごとに使用有効期限内であるかどうかを判断することを特徴とする請求項１９に記載の可搬型メディアとネットワークの連携装置。
【請求項２２】　可搬型メディアが、メディア活用情報に加え、データ暗号化鍵によって暗号化された暗号化データを更に記録し、
第１の電子計算機が、利用者ごとの秘密情報を格納する第１の秘密情報格納手段と、前記暗号化データをデータ暗号化鍵を用いて復号化しデータを生成する第１のデータ復号化手段と、前記利用者ごとの秘密情報を用いて復号化する第２のデータ復号化手段とを更に備え、
第２の電子計算機が、前記暗号化データの暗号化に用いたデータ暗号化鍵を管理する可搬型メディア情報管理手段と、前記利用者ごとの秘密情報と一対の公開情報を管理する利用者情報管理手段と、前記公開情報を用いてデータ暗号化鍵を暗号化して暗号化データ暗号化鍵を生成するデータ暗号化手段とを更に備え、
前記公開情報と前記秘密情報とは、公開情報を用いてデータを変換すると、秘密情報を用いてしか復元できない関係にあり、
前記可搬型メディアの使用有効期限内である場合、前記暗号化手段によって生成された暗号化データ暗号化鍵を第１の電子計算機から第２の電子計算機に送信した後、前記第２のデータ復号化手段が前記暗号化データ暗号化鍵を復号化してデータ暗号化鍵を生成することを特徴とする請求項１９又は請求項２１に記載の可搬型メディアとネットワークの連携装置。
【請求項２３】　可搬型メディアが、メディア活用情報に加え、データ暗号化鍵によって暗号化された暗号化データを更に記録し、
第１の電子計算機が、利用者ごとの秘密情報を格納する第１の秘密情報格納手段と、前記暗号化データをデータ暗号化鍵を用いて復号化しデータを生成する第１のデータ復号化手段と、前記利用者ごとの秘密情報を用いて復号化する第２のデータ復号化手段とを更に備え、
第２の電子計算機が、前記暗号化データの暗号化に用いたデータ暗号化鍵を、タイトル情報ごとに管理する可搬型メディア管理手段と、前記利用者ごとの秘密情報と一対の公開情報を管理する利用者情報管理手段と、前記公開情報を用いてデータ暗号化鍵を暗号化して暗号化データ暗号化鍵を生成するデータ暗号化手段とを更に備え、
前記公開情報と前記秘密情報とは、公開情報を用いてデ

ータを変換すると、秘密情報を用いてしか復元できない関係にあり、
第２の電子計算機の使用有効期限管理手段によって、第１の電子計算機より送信されるタイトル情報に該当する可搬型メディアが、使用有効期限内であると判断された場合にのみ、前記データ暗号化手段によって生成される暗号化データ暗号化鍵を、前記第２の電子計算機から前記第１の電子計算機へ送信し、前記第２のデータ復号化手段が前記暗号化データ暗号化鍵を復号化してデータ暗号化鍵を生成することを特徴とする、請求項１５に記載の可搬型メディアとネットワークの連携装置。
【請求項２４】　第１の電子計算機が、データを暗号化するデータ暗号化手段を更に備え、
第２の電子計算機が、それぞれに固有な秘密情報を格納する第２の秘密情報格納手段と、任意のデータに対して、その時限りの疑似変化を与える疑似変化情報を生成する疑似変化情報生成手段と、前記疑似変化情報など、情報を記憶する情報記憶手段と、データを復号化するデータ復号化手段とを更に備え、
メディア活用情報としては、前記秘密情報と一対の公開情報が少なくとも含まれており、
前記公開情報と前記秘密情報とは、公開情報を用いてデータを変換すると、秘密情報を用いてしか復元できない関係にあり、
タイトル情報を第２の電子計算機に送信する際に、前記データ暗号化手段が、第２の電子計算機の生成する疑似変化情報と前記メディア活用情報に含まれる公開鍵情報とを用いて暗号化し、
前記データ復号化手段が、前記情報記憶手段により記憶しておいた前記疑似変化情報と前記第２の秘密情報格納手段に格納されている秘密情報とを用いて前記暗号化されたタイトル情報を復号化し、
前記復号化されたタイトル情報により特定される可搬型メディアが使用有効期限内であるかどうかを判断することを特徴とする、請求項１５に記載の可搬型メディアとネットワークの連携装置。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、大量に出版される電子計算機用の可搬型メディア内に記録されている情報を、可搬型メディアの不正な利用を防止するために用いる、可搬型メディアに対するサービスの提供法、また、可搬型メディアとネットワークを連携させたサービスの提供法に関する。
【０００２】
【従来の技術】従来、電子計算機用の可搬型メディアとしてはフロッピーディスクやＣＤ－ＲＯＭ、ＰＤなどが利用されてきており、これらの不正な利用を防止するためのサービスの例として、ＣＤ－ＲＯＭのパッケージにキーコードのラベルを貼付しておき、利用開始時にこのキーコードを入力させることにより、正しく購入したものであることを利用者自身に証明させるといったものがある。

【０００３】また、ネットワークと連携したサービスとしては、特開平７－２９５６７４号公報に示すように、ＣＤ－ＲＯＭに一部暗号化されたデータを入れておき、ネットワーク等で別途入手する復号用の鍵でデータを解読して用い、同時に課金を行うシステムが提供されている。この方法について以下に簡単に説明する。

【０００４】まず、そのセッションに限り有効な暗号化鍵を利用者の側で生成する。次に、この暗号化鍵をデータ復号用の鍵を配布するセンター側の公開鍵で暗号化してセンターに渡し、センターではセンターの秘密鍵を用いて利用者の側で生成した暗号化鍵を復号化し、この利用者が生成した暗号化鍵を用いてＣＤ－ＲＯＭ内のデータ復号用の鍵を暗号化して利用者に送信する。この場合、センター側の公開鍵はＣＤ－ＲＯＭにあらかじめ記録されている。このようにして、データ復号用の鍵の入手を安全に行うことを可能とするものである。

【０００５】データ復号用の鍵の入手については、可搬型メディア上のデータの復号の場合に限らず、特開平７－２８８５１９号公報にあるように、公開鍵暗号方式を用いて相互に認証しながら交換する方法も提案されている。この方法について以下に簡単に説明する。
【０００６】まず、利用者側から利用者の識別番号を送信するとともにディジタル情報をセンターに要求する。センターでは、識別番号に応じて管理しているパスワード、あるいは要求の時点で生成する乱数などをセンターの秘密鍵で署名して利用者に返す。利用者の側では受けとったデータをセンターの公開鍵で認証して、通信相手が正しい相手であることを確認したうえで、解読済みのデータを利用者の秘密鍵で署名し、かつ、センターの公開鍵で暗号化してセンターに渡す。センターの側では、受けとったデータをセンターの秘密鍵で解読したうえ、さらに利用者の公開鍵で認証して、通信相手が正しい相手であることを確認したうえで、そのセッションに限り有効なセッション鍵を用いてデータを暗号化して利用者に渡す。

【０００７】また、特開平８－５４９５１号公報に示すように、可搬型メディア上に限らず、ソフトウェアの使用量を検知して、最大可能使用量を超えた場合に、その使用を阻害する方法が提案されている。この方法について以下に簡単に説明する。
【０００８】ソフトウェアの使用量を管理する手段を設け、ソフトウェアの使用量を検知し、予め定められた使用量に達したかどうかを判断し、規定の使用量を超えた場合には、ソフトウェアの出力信号を阻害する信号を重畳するなどして、使用を阻害する。または、あらかじめ出力信号を阻害するような信号を重畳したデータを記録しておき、規定された使用量を超えていない場合には、

阻害信号をはずして出力する。

【０００９】また、一般に、試用期限が設けられたソフトウェアが配布されており、特定の期間に限って、ソフトウェアを試用することが可能で、その期間を過ぎると使用不可となるものがある。

【００１０】

【発明が解決しようとする課題】しかし、ＣＤ－ＲＯＭのパッケージにキーコードのラベルを貼付する方法では、キーコードが誰の目にも明らかであり、ＣＤ－ＲＯＭを不正に貸与した場合にでも、このキーコードを入力しさえすればＣＤ－ＲＯＭが利用できてしまうことになる。

【００１１】また、特開平７－２９５６７４号公報に示す方法では、センターの公開鍵がＣＤ－ＲＯＭの本体に記録されていることにより、公開鍵があらかじめ固定されることになり、課金処理を行うセンターを追加すると、その公開鍵を得るためには別途利用者が公開鍵取得の操作をすることが必要となるため、センターの追加のために利用者の利便性を損なう結果となる。しかし、逆に、センターの数をあらかじめ決定した数で抑えるとすると、センターが処理の集中に耐えられなくなる可能性もあり、利用者の利便性はやはり損なわれる結果となる。また、センターがクレジットカード会社を兼ねている場合には、あらかじめ固定されたセンターでしか運用しないとすると、利用者が既に持っているクレジットカードが使えない可能性があるという点で利用者の利便性を損なうものである。

【００１２】逆に、複数のセンターを設けるためには、異なる金型を作成してＣＤ－ＲＯＭをプレスする必要があり、その結果、コスト高を招くことになる。また、データ復号用の鍵を暗号化する特定セッション用の暗号化鍵を利用者側で生成してセンターに送る方法では、利用者認証が行なえず、ＣＤ－ＲＯＭを不正に貸与する可能性を排除できない。

【００１３】特開平７－２８８５１９号公報では、利用者・センターの相互の認証の問題は解決されているが、センターの公開鍵を利用者側で得る方法については記述されていない。

【００１４】また、特開平８－５４９５１号公報にあるような方法では、利用者がこの方式によらずデータにアクセスすれば使用量を超えてもデータの利用が可能になるという可能性があるとともに、この方式によらなければアクセスできない形式のデータのみを提供することになるとすれば、汎用性に欠けるデータを配布することになる。

【００１５】また、ソフトウェアの試用期間を限定する現在の方法では、パソコン側の時計を過去に戻したり、再度試用ソフトウェアをインストールしなおしたりといった方法で、再度試用可能な状態にすることができてしまい、事実上、特定期間に限定することが不可能である。

【００１６】本発明は、上記問題点に鑑み、可搬型メディアを単独で、あるいはネットワークと連携して用いる場合に、その不正使用を排除することを目的としてなされたものである。

【００１７】

【課題を解決するための手段】上記の課題を解決するために、本発明は、第１に、大容量のデータの記録が可能な可搬型メディア内の暗号化データを復号化するのに必要なデータ暗号化鍵を利用者ごとの秘密情報で解読可能な形式で暗号化して、暗号化データ暗号化鍵とし、この暗号化データ暗号化鍵を、該可搬型メディアそれぞれに固有なメディア活用情報として記録しておき、利用者ごとの秘密情報は別途格納しておくことを特徴とする可搬型メディアの駆動装置であり、可搬型メディア内の暗号化データを復号化する際には、まず利用者ごとの秘密情報を得て、これによって可搬型メディアのメディア活用情報内の暗号化データ暗号化鍵を復号化してデータ暗号化鍵とし、さらにこのデータ暗号化鍵によって可搬型メディア内の暗号化データを復号化する構成としたものである。

【００１８】これにより、可搬型メディアを利用できるのは、あらかじめ特定された利用者であって、かつ、利用の際には利用者ごとの秘密情報を必要とするため、可搬型メディアを単独では利用することができず、結果として不正な利用を防止し、さらに、メディア活用情報まで含めて不正に複製しても特定された利用者の秘密情報がなければ利用できないため、結果として不正な複製を防止するという効果を奏するものである。

【００１９】また、本発明は、第２に、大容量のデータの記録が可能な可搬型メディア内の暗号化データを復号化するのに必要なデータ暗号化鍵を、可搬型メディアのメディア活用情報に記録されているタイトル情報ごとにサーバ側で管理しておき、また、利用者の秘密情報と一対の公開の情報を前記タイトル情報とタイトル情報ごとの発行番号情報ごとにサーバ側で管理しておき、利用者の秘密情報は別途格納しておいてクライアント側で利用することを特徴とする可搬型メディアとネットワークの連携装置であり、利用者はメディア活用情報に記録されているタイトル情報と発行番号情報をサーバ側に通知してデータ暗号化鍵の取得を依頼し、サーバ側は得られたタイトル情報に対応するデータ暗号化鍵を、得られたタイトル情報と発行番号情報に対応する公開の情報と、別途発生させる乱数などを用いて暗号化して送り返し、利用者側では利用者ごとの秘密情報を用いて、得られたデータから乱数を分離し、さらにデータ暗号化鍵を得て、暗号化データを復号化して利用する構成としたものである。

【００２０】これにより、可搬型メディアを利用できるのは、タイトル情報・発行番号情報と、利用者の保持す

る秘密情報と一対の公開の情報を登録済みの特定された利用者であって、かつ、利用の際には利用者ごとの秘密情報を必要とするため、可搬型メディアを単独では利用することができず、結果として不正な利用を防止し、さらに、メディア活用情報まで含めて不正に複製しても特定された利用者の秘密情報がなければ利用できないため、結果として不正な複製を防止するとともに悪意の利用者のなりすましを防止できるという効果をも奏するものである。

【００２１】また、本発明は、第３に、可搬型メディアのメディア活用情報にサーバの秘密情報と一対の公開情報を記録しておき、サーバの秘密情報は別途格納しておいてサーバ側で利用することを特徴とする可搬型メディアとネットワークの連携装置であり、利用者からサーバにデータを送信する際には、サーバで別途発生させる乱数などと、メディア活用情報内の公開情報を用いて暗号化して送信し、サーバ側では、サーバの秘密情報と前記乱数を用いて得られたデータの正当性を確認したのち、乱数を分離して、利用者からデータを得る構成としたものである。

【００２２】これにより、利用者からサーバに安全にデータを送信する際に必要とする、サーバの公開鍵の取得が容易であるという効果を奏するものであり、かつ、サーバの公開鍵が可搬型メディアごとに異なるものであっても良いという効果を奏するものである。

【００２３】また、本発明は、第４に、可搬型メディアそれぞれに固有のメディア活用情報としてタイトル情報とタイトル情報ごとの発行番号情報を設け、このタイトル情報と発行番号情報とを用いてサーバ側で可搬型メディアの使用量を管理することを特徴とする可搬型メディアとネットワークの連携装置であり、可搬型メディアを利用する際には、メディア活用情報内のタイトル情報と発行番号情報とをサーバに送信し、サーバ側では該可搬型メディアの使用量を加算したり、また、最大使用量が設定されている場合には、それを超えるかどうかの判断を行なう構成としたものである。

【００２４】これにより、該可搬型メディアの使用量をもとに利用料金を利用者に対して請求したり、また、あらかじめ利用料金を払い込んである場合に、それに応じた最大使用量を超える場合にはその旨通知したりといったことが可能であって、可搬型メディアの無制限な利用を防止するという効果を奏するものである。

【００２５】また、本発明は、第５に、前記第２の構成と前記第４の構成とを組合せた可搬型メディアとネットワークの連携装置であり、常にデータ暗号化鍵をサーバから取得するようにし、最大使用量を超える場合にはデータ暗号化鍵を渡さないようにする構成としたものである。

【００２６】これにより、最大使用量を超えての可搬型メディアの無制限な利用を確実に防止するという効果を奏するものである。

【００２７】また、本発明は、第６に、前記第３の構成と前記第５の構成とを組合せた可搬型メディアとネットワークの連携装置であり、データ暗号化鍵取得のためのメディア活用情報を暗号化して送信する構成としたものである。

【００２８】これにより、メディア活用情報に記述されている情報を安全にサーバに送信することが可能であるという効果を奏するものである。

【００２９】また、本発明は、第７に、可搬型メディアそれぞれに固有のメディア活用情報として使用有効期限情報を設け、サーバ側には使用有効期限を判断する手段を設けたことを特徴とする可搬型メディアとネットワークの連携装置、あるいは、可搬型メディアそれぞれに固有のメディア活用情報としてタイトル情報、あるいはタイトル情報とタイトル情報ごとの発行番号情報とを設け、サーバ側にはタイトル情報、あるいはタイトル情報とタイトル情報ごとの発行番号情報とによって該可搬型メディアの使用有効期限を管理する手段と、使用有効期限を判断する手段を設けたことを特徴とする可搬型メディアとネットワークの連携装置であって、可搬型メディアを利用する際には、メディア活用情報内の使用有効期限情報、あるいはタイトル情報、あるいはタイトル情報と発行番号情報とをサーバに送信し、サーバ側で該可搬型メディアが使用可能かどうかを判断することを特徴としたものである。

【００３０】これにより、可搬型メディアに対してあらかじめ使用有効期限を設定した場合に、それを超えて該可搬型を利用しようとする場合にその旨通知したり、また、あらかじめ利用料金を払い込んである場合に、それに応じた利用期間を超える場合にはその旨通知したりといったことが可能であって、可搬型メディアの無制限な利用を防止するという効果を奏するものである。

【００３１】また、本発明は、第８に、前記第２の構成と前記第７の構成とを組合せた可搬型メディアとネットワークの連携装置であり、常にデータ暗号化鍵をサーバから取得するようにし、使用有効期限を超える場合にはデータ暗号化鍵を渡さないようにする構成としたものである。

【００３２】これにより、使用有効期限を超えての可搬型メディアの無制限な利用を確実に防止するという効果を奏するものである。

【００３３】また、本発明は、第９に、前記第３の構成と前記第８の構成とを組合せた可搬型メディアとネットワークの連携装置であり、データ暗号化鍵取得のためのメディア活用情報を暗号化して送信する構成としたものである。

【００３４】これにより、メディア活用情報に記述されている情報を安全にサーバに送信することが可能であるという効果を奏するものである。

【００３５】

【発明の実施の形態】以下、本発明の実施の形態について、図１から図４９を用いて説明する。

【００３６】（実施の形態１）まず、請求項１及び２に対応する第１の実施の形態について説明する．図１は、本実施の形態における、可搬型メディアとして映画作品を記録した、映画作品再生システムの構成を示す図である。ここでは可搬型メディアとしては読み出し専用型ディジタル・ヴァーサタイル・ディスク（Digital Versatile Disk、以下ＤＶＤと略す）を用い、可搬型メディアそれぞれに固有であるメディア活用情報は、ＤＶＤ内の本来の記録領域とは異なる、ＤＶＤ上の専用の箇所に記録する。この専用の箇所のことをメディア活用情報記録領域と今後称する。図１において、１００はＤＶＤ再生装置である。１０１はＤＶＤ再生装置１００の動作全体を制御する中央制御手段、１０２はＤＶＤ再生装置１００に対して利用者が入力を行なうキーボードやマウス、音声認識装置、タブレット、ペン、ボタン、リモートコントロールボタンなどの入力手段、１０３は利用者に対してＤＶＤ再生装置１００が表示を行なうためのディスプレイ、スピーカなどの情報表示手段である。１０６は映画作品をデータ暗号化鍵Ｄで暗号化して記録した映画作品ＤＶＤであって、そのメディア活用情報記録領域には、映画作品の暗号化に用いたデータ暗号化鍵Ｄを、公開鍵暗号方式における利用者の公開鍵によって暗号化した暗号化データ暗号化鍵が記録されている。１０７は映画作品ＤＶＤ１０６を駆動するＤＶＤ駆動手段である。１０８は前記データ暗号化鍵Ｄを用いて映画作品ＤＶＤ１０６内の暗号化された映画作品を復号化するＤＶＤ内データ復号化手段である。１０９は公開鍵暗号方式における、前記利用者の公開鍵に対応する利用者の秘密鍵が記録されているＩＣカード、１１０はＩＣカード１０９を駆動するＩＣカード駆動手段である。１１１は前記利用者の秘密鍵を用いて、前記暗号化データ暗号化鍵を復号化してデータ暗号化鍵Ｄを生成するデータ暗号化鍵復号化手段である。

【００３７】図２は、本実施の形態におけるメディア活用情報の構成例である。図２において、２００はそれぞれに固有なメディア活用情報、２０３はメディア活用情報２００のうち、前記暗号化データ暗号化鍵Ｄに関する情報を含むデータ暗号化鍵情報であり、映画作品ＤＶＤ配布時には既にそのメディア活用情報記録領域に記録済みである。

【００３８】図３は本実施の形態の処理の流れを示すフローチャートである。以下、図１から図３を用いて本実施の形態の動作を説明する。

【００３９】利用者は書店や通信販売で購入、あるいは会員制のサービスによって配布してもらうことにより映画作品ＤＶＤ１０６を入手する。特に、書店や通信販売による場合は、メディア活用情報記録領域に、利用者の公開鍵で暗号化したデータ暗号化鍵Ｄを記録してもらったうえで購入する。会員制のサービスの場合には、あらかじめ公開鍵を登録して入会することにより、データ暗号化鍵Ｄを利用者の公開鍵で暗号化したものメディア活用情報記録領域に記録した上で、配布してもらうことが容易に行なえる。

【００４０】以降、利用者が映画作品ＤＶＤを再生する場合について、図３のフローチャートに沿って説明する。なお、図３においては角の丸い長方形で囲われた部分は、フローチャートの開始・終了を示し、長方形で囲われた部分は処理を示し、矢印は処理の流れを示している。

【００４１】図３において、まず、利用者は、映画作品ＤＶＤ１０６をＤＶＤ再生装置１００のＤＶＤ駆動手段１０７にセットし、入力手段１０２を用いて、再生開始をＤＶＤ再生装置１００の中央制御手段１０１に指示する。これにより、開始３００に示すように、映画作品ＤＶＤの再生が開始される。

【００４２】次に、ステップ３０１に示すように、中央制御手段１０１は映画作品ＤＶＤ再生開始の指示を受け付け、ステップ３０２に進む。

【００４３】次に、ステップ３０２に示すように、中央制御手段１０１の指示に従い、ＤＶＤ駆動手段１０７は、映画作品ＤＶＤ１０６のメディア活用情報記録領域から、データ暗号化鍵情報２０３を得て、ステップ３０３に進む。このデータ暗号化鍵情報２０３の中には、映画作品ＤＶＤ内の映画作品の暗号化に用いたデータ暗号化鍵Ｄを、利用者の公開鍵で暗号化した、暗号化データ暗号化鍵が入っている。

【００４４】次に、ステップ３０３に示すように、中央制御手段１０１の指示に従い、ＩＣカード駆動手段１１０は、ＩＣカード１０９に格納されている利用者の秘密鍵ＳＵを得て、ステップ３０４に進む。

【００４５】次に、ステップ３０４に示すように、中央制御手段１０.1の指示に従い、データ暗号化鍵復号化手段１１１は、既に得た利用者の秘密鍵ＳＵを用いて、データ暗号化鍵情報２０３に入っている暗号化データ暗号化鍵を復号化し、データ暗号化鍵Ｄを得て、ステップ３０５に進む。

【００４６】次に、ステップ３０５に示すように、中央制御手段１０１の指示に従い、ＤＶＤ内データ復号化手段１０８は、既に得たデータ暗号化鍵Ｄを用いて、映画作品ＤＶＤ１０６上の暗号化されているデータを復号化し、情報表示手段１０３によって利用者に表示し、終了３０６へ進む。

【００４７】なお、本実施の形態においては可搬型メディアとしてＤＶＤ、メディア活用情報の記録領域としてＤＶＤ上のメディア活用情報記録領域を用いたが、可搬型メディアとしてフロッピーディスクやＰＤ、ＣＤ－ＲＯＭなどの他のメディアや、書換え可能型のＤＶＤを用

い、メディア活用情報の記録領域については、メディア本体の記録領域を用いることも可能である。

【００４８】また、本実施の形態においては、利用者の秘密鍵をＩＣカードに格納する例について示したが、ＩＣカードへのアクセス時には、ＩＣカード自身に設けられているパスワードなどを別途用いて、利用者以外の第三者からのアクセスを排除することも可能である。さらに、利用者の秘密鍵はＩＣカードに格納するのではなく、ＤＶＤ再生装置自身の記憶領域に暗号化して記録しておき、利用者のパスワード入力などによって復号化して利用するといった形態や、磁気カードに記録しておくといった形態、利用者自身が覚えておいて、都度入力するといった形態も可能である。

【００４９】また、本実施の形態においては特に述べなかったが、映画作品ＤＶＤの中に複数の映画作品が記録されている場合に、データ暗号化鍵を映画作品ごとに設けることも可能である。その場合には、それぞれのデータ暗号化鍵を利用者の公開鍵で暗号化し、暗号化データ暗号化鍵をメディア活用情報記録領域に記録することになる。

【００５０】また、本実施の形態においては、利用者を一人であると仮定していたが、家族など、複数の利用者が映画作品ＤＶＤを利用するということがあらかじめ分かっている場合には、複数の利用者それぞれの公開鍵によってデータ暗号化鍵を暗号化し、メディア活用情報記録領域に記録することによって、それぞれの利用者による映画作品ＤＶＤの利用を可能とすることができる。

【００５１】また、本実施の形態においては特に述べなかったが、データ暗号化鍵や利用者の秘密鍵の漏洩を防止するために、ＩＣカード駆動手段１１０、データ暗号化鍵復号化手段１１１は、情報表示手段１０３を実現するハードウェアに組み込むことによって実装してもよい。

【００５２】以上のように、本実施の形態では、可搬型メディアを利用できるのは、あらかじめ特定された利用者であって、かつ、利用の際には利用者ごとの秘密情報を必要とするため、可搬型メディアを単独では利用することができず、結果として不正な利用を防止し、さらに、メディア活用情報まで含めて不正に複製しても特定された利用者の秘密情報がなければ利用できないため、結果として不正な複製を防止できる。

【００５３】また、メディア活用情報は、可搬型メディアの金型でプレスするものではないため、大量に同一の内容を持つ可搬型メディアをプレスしたあとに、一枚ごとにメディア活用情報を記録することで、暗号化データのプレスのためには共通の金型を用いることができるというコスト低下にもつながり、その実用的効果は大きい。

【００５４】（実施の形態２）次に、請求項３乃至５に対応する第２の実施の形態について説明する．図４は、本実施の形態における、可搬型メディアとして映画作品を記録した、映画作品再生システムの構成を示す図である。なお、可搬型メディアとしては実施の形態１と同じ、読み出し専用型ＤＶＤを用いるものとする。

【００５５】図４において、４００はＤＶＤ再生装置である。４０１はＤＶＤ再生装置４００の動作全体を制御する中央制御手段、４０２はＤＶＤ再生装置４００に対して利用者が力を行なうキーボードやマウス、音声認識装置、タブレット、ペン、ボタン、リモートコントロールボタンなどの入力手段、４０３は利用者に対してＤＶＤ再生装置４００が表示を行なうためのディスプレイ、スピーカなどの情報表示手段、４０４はＤＶＤ再生装置４００のネットワークに対する情報の送受信を行なう情報送受信手段である。４０６は映画作品をデータ暗号化鍵Ｄで暗号化して記録した映画作品ＤＶＤであって、そのメディア活用情報記録領域には、映画作品ＤＶＤの種類を特定可能なタイトル情報と、タイトル情報ごとの発行番号情報が記録されている。４０７は映画作品ＤＶＤ４０６を駆動するＤＶＤ駆動手段である。４０８はデータ暗号化鍵Ｄを用いて前記映画作品ＤＶＤ４０６内の暗号化された映画作品を復号化するＤＶＤ内データ復号化手段である。４０９は公開鍵暗号方式における、前記利用者の公開鍵に対応する利用者の秘密鍵が記録されているＩＣカード、４１０はＩＣカード４０９を駆動するＩＣカード駆動手段である。４１１は前記利用者の秘密鍵を用いて、送信データ暗号化手段４３２によって生成される暗号化データ暗号化鍵を復号化してデータ暗号化鍵Ｄを生成するデータ暗号化鍵復号化手段である。

【００５６】４２０は映画作品ＤＶＤ４０６に記録されている映画作品の暗号化に用いたデータ暗号化鍵を管理し、利用者の要求に応じてデータ暗号化鍵を配布する鍵管理サーバである。４２１は前記鍵管理サーバ４２０の動作全体を制御する中央制御手段、４２４は鍵管理サーバ４２０のネットワークに対する情報の送受信を行なう情報送受信手段である。４３２は利用者に対して送信するデータ暗号化鍵を公開鍵暗号方式における利用者の公開鍵で暗号化する、すなわち暗号化データ暗号化鍵を生成する送信データ暗号化手段、４３３は送信データ暗号化手段において利用する乱数を発生させる乱数発生手段、４３４は利用者の公開鍵を、前記タイトル情報と前記発行番号情報によって管理する利用者情報管理手段、４３５は前記データ暗号化鍵を前記タイトル情報によって管理するＤＶＤ情報管理手段である。４４０はＤＶＤ再生装置４００と鍵管理サーバ４２０との間を繋ぐネットワークである。

【００５７】図５は、本実施の形態にかかわるメディア活用情報の構成例である．図５において、５００はそれぞれに固有なメディア活用情報、メディア活用情報５００のうち、５０１は映画作品ＤＶＤの種類を特定可能なタイトル情報、５０２は該映画作品ＤＶＤを他のものと

識別可能な、前記タイトル情報ごとの発行番号情報であり、映画作品ＤＶＤ配布時には既に、前記メディア活用情報記録領域に記録済みである。

【００５８】図６は、本実施の形態にかかわる利用者情報の構成例である．図６において、６００は利用者情報、６０１はメディア活用情報５００に含まれるタイトル情報、６０２はメディア活用情報５００に含まれる発行番号情報、６０３はタイトル情報６０１と発行番号情報６０２とで特定可能な映画作品ＤＶＤを保有している利用者の、公開鍵暗号方式における公開鍵を含む、利用者公開鍵情報である。なお、ここでは、一つのエントリのみ示したが、実際には、このような形式で複数のエントリが存在する。これらは利用者情報管理手段４３４によって管理されている。

【００５９】図７は、本実施の形態にかかわるＤＶＤ情報の構成例である。図７において、７００はＤＶＤ情報、７０１はメディア活用情報５００内に含まれるタイトル情報、７０２はこのタイトル情報７０１によって特定可能な種類の映画作品ＤＶＤ内に記録されている映画作品を暗号化するのに用いたデータ暗号化鍵Ｄを含むデータ暗号化鍵情報である。なお、ここでは、一つのエントリのみ示したが、実際には、このような形式で複数のエントリが存在する。これらはＤＶＤ情報管理手段４３５によって管理されている。

【００６０】図８は本実施の形態の処理の流れを示すフローチャートである。以下、図４から図８を用いて本実施の形態の動作を説明する。

【００６１】利用者は書店や通信販売で購入、あるいは会員制のサービスによって配布してもらうことにより映画作品ＤＶＤ４０６を入手する。以降、利用者が映画作品ＤＶＤを再生する場合について、図８のフローチャートに沿って説明する。なお、図８においては角の丸い長方形で囲われた部分は、フローチャートの開始・終了を示し、長方形で囲われた部分は処理を示し、矢印は処理の流れを示している。

【００６２】まず、利用者は、映画作品ＤＶＤ４０６をＤＶＤ再生装置４００のＤＶＤ駆動手段４０７にセットし、入力手段４０２を用いて、再生開始をＤＶＤ再生装置４００の中央制御手段４０１に指示する。これにより、開始８００に示すように、映画作品ＤＶＤの再生が開始される。

【００６３】次に、ステップ８０１に示すように、ＤＶＤ再生装置４００の中央制御手段４０１は映画作品ＤＶＤ再生開始の指示を受け付け、ＤＶＤ駆動手段４０７によって映画作品ＤＶＤ４０６のメディア活用情報５００のうち、タイトル情報５０１と発行番号情報５０２とを得て、これらを情報送受信手段４０４により、ネットワーク４４０を経由して鍵管理サーバ４２０に送信し、暗号化データ暗号化鍵の取得を依頼し、ステップ８０２に進む。

【００６４】次に、ステップ８０２に示すように、鍵管理サーバ４２０の中央制御手段４２１は、暗号化データ暗号化鍵取得依頼の指示を、タイトル情報５０１と発行番号情報５０２とともに情報送受信手段４２４により受信し、ＤＶＤ情報管理手段４３５によって、タイトル情報５０１を元に、データ暗号化鍵情報７０２を得て、ステップ８０３に進む。ここで、ＤＶＤ情報７００のうちのタイトル情報７０１は、前記タイトル情報５０１と等しい値を持つ。

【００６５】次に、ステップ８０３に示すように、利用者情報管理手段４３４によって、タイトル情報５０１と発行番号情報５０２とを元に、利用者公開鍵情報６０３を得て、ステップ８０４に進む。ここで、利用者情報６００のうちのタイトル情報６０１と発行番号情報６０２とは、それぞれ前記タイトル情報５０１と前記発行番号情報５０２とに等しい。

【００６６】次に、ステップ８０４に示すように、乱数発生手段４３３により、乱数Ｒを発生させ、ステップ８０５に進む。

【００６７】次に、ステップ８０５に示すように、送信データ暗号化手段４３２において、前記乱数Ｒを用いて、前記データ暗号化鍵情報７０２に含まれているデータ暗号化鍵Ｄを暗号化し、さらに、Ｒと前記暗号化されたＤとを組合せたデータを前記利用者公開鍵情報６０３に含まれている利用者公開鍵ＰＵによって暗号化し、その結果を、情報送受信手段４２４により、ネットワーク４４０を経由してＤＶＤ再生装置４００に送信し、ステップ８０６に進む。ここで、乱数Ｒと利用者公開鍵ＰＵによる暗号化の関数を、それぞれｅ１、ｅ２として、暗号化の様子を模式的に表すと、ＤＶＤ再生装置４００に送信されるデータは次の（数１）のようになる。ｅ１、ｅ２の引数は、それぞれ、一つ目の引数が暗号化鍵、二つ目の引数が暗号化されるデータである。

【００６８】

【数１】ｅ２（ＰＵ，Ｒ＋ｅ１（Ｒ，Ｄ））

次に、ステップ８０６に示すように、ＤＶＤ再生装置４００は情報送受信手段４０４により鍵管理サーバ４２０からの（数１）で示されるデータを受信し、さらに、中央制御手段４０１の指示に従い、ＩＣカード駆動手段４１０は、ＩＣカード４０９に格納されている利用者秘密鍵ＳＵを得て、データ暗号化鍵復号化手段４１１により、データ暗号化鍵Ｄを得て、ステップ８０７に進む。ここで、乱数Ｒと利用者秘密鍵ＳＵによる復号化の関数を、それぞれｄ１、ｄ２として、復号化の様子を模式的に表すと、データ暗号化鍵復号化手段の動作は以下の（数４）から（数５）のように表される。ｄ１、ｄ２の引数は、それぞれ、一つ目の引数が暗号化鍵、二つ目の引数が復号化されるデータであり、前記暗号化の関数ｅ１、ｅ２とは、逆の関係にあり、それぞれ（数２）と（数３）に示すような関係がある。この式に現れるＸ、

Ｙは暗号化される対象のデータを示す変数である。

【００６９】

【数２】ｄ１（Ｒ，ｅ１（Ｒ，Ｘ））＝Ｘ

【００７０】

【数３】ｄ２（ＳＵ，ｅ２（ＰＵ，Ｙ））＝Ｙ

【００７１】

【数４】ｄ２（ＳＵ，ｅ２（ＰＵ，Ｒ＋ｅ１（Ｒ，Ｄ））））＝Ｒ＋ｅ１（Ｒ，Ｄ）

【００７２】

【数５】ｄ１（Ｒ，ｅ１（Ｒ，Ｄ））＝Ｄ

次に、ステップ８０７に示すように、ＤＶＤ内データ復号化手段４０８は、既に得たデータ暗号化鍵Ｄを用いて、映画作品ＤＶＤ４０６の暗号化されているデータを復号化し、情報表示手段４０３によって利用者に表示し、終了８０６へ進む。

【００７３】なお、本実施の形態においては可搬型メディアとしてＤＶＤ、メディア活用情報の記録領域としてＤＶＤ上のメディア活用情報記録領域を用いたが、可搬型メディアとしてフロッピーディスクやＰＤ、ＣＤ－ＲＯＭなどの他のメディアや、書換え可能型のＤＶＤを用い、メディア活用情報の記録領域については、メディア本体の記録領域を用いることも可能である。

【００７４】また、本実施の形態においては、利用者の秘密鍵をＩＣカードに格納する例について示したが、ＩＣカードへのアクセス時には、ＩＣカード自身に設けられているパスワードなどを別途用いて、利用者以外の第三者からのアクセスを排除することも可能である。さらに、利用者の秘密鍵はＩＣカードに格納するのではなく、ＤＶＤ再生装置自身の記憶領域に暗号化して記録しておき、利用者のパスワード入力などによって復号化して利用するといった形態や、磁気カードに記録しておくといった形態、利用者自身が覚えておいて、都度入力するといった形態も可能である。

【００７５】また、本実施の形態においては特に述べなかったが、映画作品ＤＶＤの中に複数の映画作品が記録されている場合に、データ暗号化鍵を映画作品ごとに設けることも可能である。その場合には、ＤＶＤ情報のエントリとしては、タイトル情報とともにＤＶＤ内の映画作品を区別する情報でデータ暗号化鍵を管理し、ＤＶＤ再生装置からデータ暗号化鍵の取得を依頼する場合にも、ＤＶＤ内の映画作品を区別する情報をともに鍵管理サーバに送信することになる。

【００７６】また、本実施の形態においては、利用者を一人であると仮定していたが、家族など、複数の利用者が映画作品ＤＶＤを利用するということがあらかじめ分かっている場合には、複数の利用者それぞれの公開鍵を利用者情報として管理し、複数の発行番号情報を一枚の映画作品ＤＶＤに設けることで、利用者を特定したり、あるいは、一つの発行番号情報に対して一定の個数まで利用者を設定できるようにして、何番目の利用者であるかという情報をもとに利用者を特定したりといった方法で、利用者公開鍵を取得するようにし、それぞれの利用者による映画作品ＤＶＤの利用を可能とすることができる。

【００７７】また、本実施の形態においては特に述べなかったが、データ暗号化鍵・利用者の秘密鍵の漏洩を防止するために、ＩＣカード駆動手段４１０、データ暗号化鍵復号化手段４１１は、情報表示手段４０３を実現するハードウェアに組み込むことによって実装してもよい。

【００７８】また、本実施の形態においては特に述べなかったが、鍵管理サーバ自身の認証を行なうために、鍵管理サーバの秘密鍵を用いた公開鍵暗号方式における署名を前記（数１）で示されるデータに施し、ともにＤＶＤ再生装置に送信し、ＤＶＤ再生装置では、鍵管理サーバの公開鍵を用いることで、鍵管理サーバの署名を認証したのち、前記（数４）と前記（数５）に示す方法でデータ暗号化鍵を取得するといった形態も可能である。

【００７９】また、本実施の形態では、その時限りの疑似変化を与えることのできる疑似変化情報として乱数を用いたが、これに限ったわけではなく、クレジットカード番号などを暗号化した場合に、クレジットカード自身は解読できないにしても、暗号化した結果が一定とならないように、更にその時限りの疑似変化を与えられるものならば一向に構わない。

【００８０】以上のように、本実施の形態では、可搬型メディアを利用できるのは、タイトル情報ごとの発行番号情報に対して、利用者の保持する秘密鍵と一対の公開鍵を登録済みの特定された利用者であって、かつ、利用の際には利用者ごとの秘密鍵を必要とするため、可搬型メディアを単独では利用することができず、結果として不正な利用を防止し、さらに、メディア活用情報まで含めて不正に複製しても特定された利用者の秘密情報がなければ利用できないため、結果として不正な複製を防止するとともに悪意の利用者のなりすましを防止できる。

【００８１】また、サーバ認証のステップがないためシステム構成が簡単になるとともに悪意のサーバのなりすましに対してもタイトル情報と発行番号情報が漏洩するのみで済む。

【００８２】更に、メディア活用情報は、可搬型メディアの金型でプレスするものではないため、大量に同一の内容を持つ可搬型メディアをプレスしたあとに、一枚ごとにメディア活用情報を記録することで、暗号化データのプレスのためには共通の金型を用いることができるというコスト低下など、その実用的効果は大きい。

【００８３】（実施の形態３）次に、請求項６及び７に対応する第３の実施の形態について説明する．図９は、本実施の形態による、可搬型メディアとして映画作品を記録した、視聴の都度対価の支払いを行なう映画作品再生システムの構成を示す図である。

【００８４】また、料金の支払はクレジットカードにより行い、視聴の都度、料金サーバに視聴料金を問合せた上でクレジットカード番号を通知することにより、クレジットカード番号を総武する。なお、クレジットカード番号は、視聴の都度料金サーバに対して通知するものとする。

【００８５】図９において、９００はＤＶＤ再生装置である。９０１は前記ＤＶＤ再生装置９００の動作全体を制御する中央制御手段、９０２は前記ＤＶＤ再生装置９００に対して利用者が入力を行なうキーボードやマウス、音声認識装置、タブレット、ペン、ボタン、リモートコントロールボタンなどの入力手段、９０３は利用者に対して前記ＤＶＤ再生装置９００が表示を行なうためのディスプレイ、スピーカなどの情報表示手段、９０４は前記ＤＶＤ再生装置９００のネットワークに対する情報の送受信を行なう情報送受信手段、９０５は前記情報送受信手段９０４などから得られる情報を一時的に記憶しておく情報記憶手段である。９０６は映画作品をデータ暗号化鍵Ｄで暗号化して記録した映画作品ＤＶＤであって、そのメディア活用情報記録領域には、映画作品ＤＶＤの種類を特定可能なタイトル情報と、料金サーバの、公開鍵暗号方式における公開鍵が記録されている。９０７は前記映画作品ＤＶＤ９０６を駆動するＤＶＤ駆動手段である。９１２はクレジットカード番号を料金サーバに送信する際に、クレジットカード番号を、料金サーバの公開鍵を用いて暗号化し、暗号化クレジットカード番号とする、送信データ暗号化手段である。

【００８６】９２０は映画作品ＤＶＤ９０６に記録されている映画作品の視聴料金を徴収する料金サーバである。９２１は前記料金サーバ２０の動作全体を制御する中央制御手段、９２４は前記料金サーバ９２０のネットワークに対する情報の送受信を行なう情報送受信手段、９２５は前記情報送受信手段９２４などから得られる情報や、料金サーバ９２０自身で生成した情報を一時的に記憶しておく情報記憶手段である。９２９は公開鍵暗号方式における、前記料金サーバの公開鍵に対応する料金サーバの秘密鍵が記録されているＩＣカード、９３０は前記ＩＣカード９２９を駆動するＩＣカード駆動手段である。９３１は前記料金サーバの秘密鍵を用いて、前記暗号化クレジットカード番号を復号化して、クレジットカード番号を生成する受信データ復号化手段である。９３３は前記送信データ暗号化手段９１２において利用する乱数を発生させる乱数発生手段、９３５は映画作品ＤＶＤを再生する場合に請求される料金を前記タイトル情報によって管理するＤＶＤ情報管理手段である。９４０は前記ＤＶＤ再生装置９００と前記料金サーバ９２０との間を繋ぐネットワークである。９５０は前記料金サーバ９２０以外の、他の料金サーバ群、９５１は前記料金サーバ群９５０に属する複数の料金サーバと前記料金サーバ９２０とを合わせた全体を示している。

【００８７】図１０は、本実施の形態にかかわるメディア活用情報の構成例である．図１０において、１０００はメディア活用情報、メディア活用情報１０００のうち、１００１は映画作品ＤＶＤの種類を特定可能なタイトル情報、１００４は料金サーバの、公開鍵暗号方式における公開鍵と、料金サーバ自身を特定する情報として、電話番号やネットワークアドレスを含む、料金サーバ公開鍵情報であり、映画作品ＤＶＤ配布時には既に前記メディア活用情報記録領域に記録済みである。

【００８８】図１１は、本実施の形態にかかわるＤＶＤ情報の構成例である．図１１において、１１００はＤＶＤ情報、１１０１は前記メディア活用情報１０００内に含まれるタイトル情報、１１０３はこのタイトル情報１１０１によって特定可能な種類の映画作品ＤＶＤを再生する場合に請求される料金を含む料金情報である。なお、ここでは、一つのエントリのみ示したが、実際には、このような形式で複数のエントリが存在する。これらは前記ＤＶＤ情報管理手段９３５によって管理されている。

【００８９】図１２は本実施の形態の処理の流れを示すフローチャートである．以下、図９から図１２を用いて本発明の第３の実施の形態の動作を説明する．利用者は書店や通信販売で購入、あるいは会員制のサービスによって配布してもらうことにより映画作品ＤＶＤ９０６を入手する。以降、利用者が映画作品ＤＶＤを再生する場合の、クレジットカード番号の送信処理について、図１２のフローチャートに沿って説明する。なお、図１２においては角の丸い長方形で囲われた部分は、フローチャートの開始・終了を示し、長方形で囲われた部分は処理を示し、矢印は処理の流れを示している。

【００９０】まず、利用者は、映画作品ＤＶＤ９０６をＤＶＤ再生装置９００のＤＶＤ駆動手段９０７にセットし、入力手段９０２を用いて、再生開始をＤＶＤ再生装置９００の中央制御手段９０１に指示する。これにより、開始１２００に示すように、まず、料金支払いのためのクレジットカード番号の送信が開始される。

【００９１】次に、ステップ１２０１に示すように、ＤＶＤ再生装置９００の中央制御手段９０１はクレジットカード番号送信の指示を受け付け、ＤＶＤ駆動手段９０７によって映画作品ＤＶＤ９０６のメディア活用情報１０００のうち、タイトル情報１００１と料金サーバ公開鍵情報１００４とを得て、料金サーバ公開鍵情報１００４から料金サーバを特定し、タイトル情報１００１を、情報送受信手段９０４により、ネットワーク９４０を経由して、特定された料金サーバに対して送信し、まず乱数と料金情報との取得を依頼し、ステップ１２０２に進む。ここで、特定される料金サーバは、説明の便宜上、料金サーバ群９５１のうちの９２０であるとし、以下の説明を続ける。

【００９２】次に、ステップ１２０２に示すように、料

金サーバ９２０の中央制御手段９２１は、乱数と料金情報との取得依頼の指示を、情報送受信手段９２４によりタイトル情報１００１とともに受信し、乱数発生手段９３３により乱数Ｒを発生させ、情報記憶手段９２５に乱数Ｒを記憶させ、ＤＶＤ情報管理手段によりタイトル情報１００１から料金情報１１０３を得て、乱数Ｒと料金情報１１０３とを、情報送受信手段９２４により、ネットワーク９４０を経由して、ＤＶＤ再生装置９００に送信し、ステップ１２０３に進む。ここで、メディア活用情報１０００内のタイトル情報１００１とＤＶＤ情報１１００内のタイトル情報１１０１とは等しいものである。

【００９３】次に、ステップ１２０３に示すように、ＤＶＤ再生装置９００の中央制御手段９０１は、乱数Ｒと料金情報１１０３とを情報送受信手段９０４により受信し、乱数Ｒは情報記憶手段９０５に記憶させ、料金情報１１０３は情報表示手段９０３に表示させたのち、入力手段９０２を利用して、利用者にクレジットカード番号Ｎを入力させ、ステップ１２０４に進む。

【００９４】次に、ステップ１２０４に示すように、送信データ暗号化手段９１２は、情報記憶手段９０５に記憶させておいた乱数Ｒと、ＤＶＤ駆動手段９０７によって映画作品ＤＶＤ９０６のメディア活用情報１０００から得られる料金サーバ公開鍵情報１００４に含まれている料金サーバ公開鍵ＰＳとを用いて、ステップ１２０３において利用者が入力したクレジットカード番号Ｎを暗号化し、ステップ１２０５に進む。ここで、ここで、乱数Ｒと料金サーバ公開鍵ＰＳによる暗号化の関数を、それぞれｅ１、ｅ２として、暗号化の様子を模式的に表すと、暗号化されたデータは次の（数６）のようになる。ｅ１、ｅ２の引数は、それぞれ、一つ目の引数が暗号化鍵、二つ目の引数が暗号化されるデータである。

【００９５】

【数６】ｅ２（ＰＳ，Ｒ＋ｅ１（Ｒ，Ｎ））

次に、ステップ１２０５に示すように、ＤＶＤ再生装置９００の中央制御手段９０１の指示により、情報送受信手段９０４により、ネットワーク９４０を経由して、料金サーバ９２０に対して、（数６）で示される、暗号化されたクレジットカード番号を送信する。

【００９６】次に、ステップ１２０６に示すように、料金サーバ９２０は情報送受信手段９２４によりＤＶＤ再生装置９００からの（数６）で示されるデータを受信し、さらに、中央制御手段９２１の指示に従い、ＩＣカード駆動手段９３０は、ＩＣカード９２９に格納されている料金サーバ秘密鍵ＳＳを得て、受信データ復号化手段９３１により、得られたデータ内の乱数Ｒが情報記憶手段９２５に記憶してある乱数と等しいことを確認した上で、クレジットカード番号Ｎを得て、終了１２０７に進む。ここで、乱数Ｒと料金サーバ秘密鍵ＳＳによる復号化の関数を、それぞれｄ１、ｄ２として、復号化の様子を模式的に表すと、受信データ復号化手段の動作は以下の（数９）から（数１０）のように表される。ｄ１、ｄ２の引数は、それぞれ、一つ目の引数が暗号化鍵、二つ目の引数が復号化されるデータであり、前記暗号化の関数ｅ１、ｅ２とは、逆の関係にあり、それぞれ（数７）と（数８）に示すような関係がある。この式に現れるＸ、Ｙは暗号化される対象のデータを示す変数である。（数９）と（数１０）との操作の間には、（数９）おいて得られる値Ｒ’が、情報記憶手段９２５に記憶してある乱数Ｒと等しいかどうかの確認を行なう。

【００９７】

【数７】ｄ１（Ｒ，ｅ１（Ｒ，Ｘ））＝Ｘ

【００９８】

【数８】ｄ２（ＳＳ，ｅ２（ＰＳ，Ｙ））＝Ｙ

【００９９】

【数９】ｄ２（ＳＳ，ｅ２（ＰＳ，Ｒ’＋ｅ１（Ｒ’，Ｎ））＝Ｒ’＋ｅ１（Ｒ’，Ｎ）

【０１００】

【数１０】ｄ１（Ｒ，ｅ１（Ｒ，Ｎ））＝Ｎ

なお、本実施の形態においては可搬型メディアとしてＤＶＤ、メディア活用情報の記録領域としてＤＶＤ上のメディア活用情報記録領域を用いたが、可搬型メディアとしてフロッピーディスクやＰＤ、ＣＤ－ＲＯＭなどの他のメディアや、書換え可能型のＤＶＤを用い、メディア活用情報の記録領域については、メディア本体の記録領域を用いることも可能である。

【０１０１】また、本実施の形態においては、料金サーバの秘密鍵をＩＣカードに格納する例について示したが、ＩＣカードへのアクセス時には、ＩＣカードに設けられているパスワードなどを別途用いて、料金サーバ管理者以外の第三者からのアクセスを排除することも可能である。さらに、料金サーバの秘密鍵はＩＣカードに格納するのではなく、料金サーバ自身の記憶領域に暗号化して記録しておき、料金サーバ管理者のパスワード入力などによって復号化して利用するといった形態や、磁気カードに記録しておくといった形態、料金サーバ管理者自身が覚えておいて、都度入力するといった形態も可能である。

【０１０２】また、本実施の形態においては特に述べなかったが、映画作品ＤＶＤの中に複数の映画作品が記録されている場合に、料金情報を映画作品ごとに設けることも可能である。その場合には、ＤＶＤ情報のエントリとしては、タイトル情報とともにＤＶＤ内の映画作品を区別する情報で料金情報を管理し、ＤＶＤ再生装置から乱数と料金情報の取得を依頼する場合にも、ＤＶＤ内の映画作品を区別する情報をともに鍵管理サーバに送信することになる。

【０１０３】また、本実施の形態においては特に述べなかったが、利用者自身の認証を行なうために、利用者の秘密鍵を用いた公開鍵暗号方式における署名を前記（数

６）で示されるデータに施し、ともに料金サーバに送信し、料金サーバでは、利用者の公開鍵を用いることで、利用者の署名を認証したのち、前記（数４）と前記（数５）に示す方法でクレジットカード番号を取得するといった形態も可能である。

【０１０４】また、本実施の形態においては特に述べなかったが、クレジットカード番号を、映画作品ＤＶＤの利用の都度、利用者に入力させるのではなく、暗号化してＤＶＤ再生装置に記憶させておき、パスワードを入力することでクレジットカード番号を送信するといった形態も可能である。

【０１０５】また、本実施の形態においては特に述べなかったが、クレジットカード番号を入力する前に、情報表示手段において表示される料金情報を見て、映画作品ＤＶＤの再生を実行するかどうかを判断し、その結果、再生を取り止める場合には、クレジットカード番号の送信も中止するといった形態も考えられる。

【０１０６】また、本実施の形態においてはメディア活用情報記録領域に記録されている料金サーバ公開鍵情報は一つであって、可搬型メディアごとに異なりうる構成としたが、複数の料金サーバ、あるいは全部の料金サーバの公開鍵情報をあらかじめメディア活用情報記録領域に記録しておくという形態も考えられる。この場合、選択する料金サーバによって異なる料金を徴収したり、一時的に料金を下げたりといった使い方も考えられる。

【０１０７】以上のように、本実施の形態では、利用者から料金サーバに安全にデータを送信する際に必要とする、料金サーバの公開鍵の取得が容易であり、かつ、料金サーバの公開鍵が可搬型メディアごとに異なるものであっても良い。

【０１０８】また、同一タイトルを含む可搬型メディアであっても公開鍵を異なるものであっても良いため、複数の料金サーバを設けることが可能で、その実用的効果は大きい。

【０１０９】（実施の形態４）次に、請求項８、９及び１０に対応する第４の実施の形態について説明する．図１３は、本発明の第４の実施の形態による、可搬型メディアとして映画作品を記録した、視聴の都度、視聴のための可搬型メディアの使用量の記録を行なう映画作品再生システムの構成を示す図である。

【０１１０】図１３において、１３００はＤＶＤ再生装置である。１３０１は前記ＤＶＤ再生装置１３００の動作全体を制御する中央制御手段、１３０２は前記ＤＶＤ再生装置１３００に対して利用者が入力を行なうキーボードやマウス、音声認識装置、タブレット、ペン、ボタン、リモートコントロールボタンなどの入力手段、１３０３は利用者に対して前記ＤＶＤ再生装置１３００が表示を行なうためのディスプレイ、スピーカなどの情報表示手段、１３０４は前記ＤＶＤ再生装置１３００のネットワークに対する情報の送受信を行なう情報送受信手段である。１３０６は映画作品を記録した映画作品ＤＶＤであって、そのメディア活用情報記録領域には、映画作品ＤＶＤの種類を特定可能なタイトル情報と、タイトル情報ごとの発行番号情報が記録されている。１３０７は前記映画作品ＤＶＤ１３０６を駆動するＤＶＤ駆動手段である。

【０１１１】１３２０は映画作品ＤＶＤ１３０６に記録されている映画作品の視聴のための可搬型メディアの使用量を記録する使用量管理サーバである。１３２１は前記使用量管理サーバ１３２０の動作全体を制御する中央制御手段、１３２４は前記使用量管理サーバ１３２０のネットワークに対する情報の送受信を行なう情報送受信手段、１３３４は映画作品ＤＶＤを再生する場合の可搬型メディアの使用量を前記タイトル情報と前記発行番号情報とによって管理する利用者情報管理手段である。１３４０は前記ＤＶＤ再生装置１３００と前記使用量管理サーバ１３２０との間を繋ぐネットワークである。

【０１１２】図１４は、本実施の形態にかかわるメディア活用情報の構成例である．図１４において、１４００はメディア活用情報、メディア活用情報１４００のうち、１４０１は映画作品ＤＶＤの種類を特定可能なタイトル情報、１４０２は該映画作品ＤＶＤを他のものと識別可能な、前記タイトル情報ごとの発行番号情報であり、映画作品ＤＶＤ配布時には既に前記メディア活用情報記録領域に記録済みである。

【０１１３】図１５は、本実施の形態にかかわる利用者情報の構成例である．図１５において、１５００は利用者情報、１５０１は前記メディア活用情報１４００内に含まれるタイトル情報、１５０２は前記メディア活用情報１４００内に含まれる発行番号情報、１５０４は前記タイトル情報１５０１と前記発行番号情報１５０２によって特定可能な可搬型メディアの使用量の累計を示す、使用量累計である。なお、ここでは、一つのエントリのみ示したが、実際には、このような形式で複数のエントリが存在する。これらは前記利用者情報管理手段１３３４によって管理されている。

【０１１４】図１６は本実施の形態の処理の流れを示すフローチャートである．以下、図１３から図１６を用いて本実施の形態の動作を説明する．利用者は書店や通信販売で購入、あるいは会員制のサービスによって配布してもらうことにより映画作品ＤＶＤ１３０６を入手する。以降、利用者が映画作品ＤＶＤを再生する場合の、使用量の管理について、図１６のフローチャートに沿って説明する。なお、図１６においては角の丸い長方形で囲われた部分は、フローチャートの開始・終了を示し、長方形で囲われた部分は処理を示し、菱形で囲われた部分は判断を示し、矢印は処理の流れを示している。

【０１１５】まず、利用者は、映画作品ＤＶＤ１３０６をＤＶＤ再生装置１３００のＤＶＤ駆動手段１３０７にセットし、入力手段１３０２を用いて、再生開始をＤＶ

Ｄ再生装置１３００の中央制御手段１３０１に指示する。これにより、開始１６００に示すように、映画作品ＤＶＤの再生処理が開始される。

【０１１６】次に、ステップ１６０１に示すように、ＤＶＤ再生装置１３００の中央制御手段１３０１は映画作品ＤＶＤ１３０６の再生開始の指示を受け付け、ＤＶＤ駆動手段１３０７によって映画作品ＤＶＤ１３０６のメディア活用情報１４００のうちタイトル情報１４０１と発行番号情報１４０２とを得て、タイトル情報１４０１と発行番号情報１４０２とを情報送受信手段１３０４により、ネットワーク１３４０を経由して、使用量管理サーバ１３２０に対して送信し、ステップ１６０２に進む。次に、ステップ１６０２に示すように、使用量管理サーバ１３２０の中央制御手段１３２１は、情報送受信手段１３２４によりタイトル情報１４０１と発行番号情報１４０２とを受信し、利用者情報管理手段１３３４に対して、タイトル情報１４０１と発行番号情報１４０２とで管理されている利用者情報の使用量累計を加算するように指示し、判断１６０３に進む。

【０１１７】次に、判断１６０３に示すように、利用者情報管理手段１３３４は、利用者情報を参照し、タイトル情報１４０１で発行番号情報１４０２の利用者情報のエントリが既に登録されているかどうかを判断する。ここで、利用者情報１５００として登録されている場合にはステップ１６０５に進み、登録されていない場合には、ステップ１６０４に進む。

【０１１８】ステップ１６０４では、利用者情報管理手段１３３４はタイトル情報１４０１で発行番号情報１４０２の利用者情報のエントリを新たに作成して登録し、ステップ１６０５に進む。説明の便宜上、この新しいエントリを以降１５００とする。

【０１１９】次に、ステップ１６０５に示すように、利用者情報管理手段１３３４は、利用者情報１５００の使用量累計１５０４に対して、新たに今回の使用量を加算し、加算された結果の使用量累計１５０４を情報送受信手段１３２４により、ネットワーク１３４０を経由して、ＤＶＤ再生装置１３００に送信し、ステップ１６０６に進む。

【０１２０】次に、ステップ１６０６に示すように、ＤＶＤ再生装置１３００の中央制御手段１３０１は、使用量累計１５０４を情報送受信手段１３０４により受信し、情報表示手段１３０３にこれを表示したうえで、映画作品ＤＶＤ１３０６の再生を開始し、終了１６０７に進む。

【０１２１】なお、本実施の形態においては可搬型メディアとしてＤＶＤ、メディア活用情報の記録領域としてＤＶＤ上のメディア活用情報記録領域を用いたが、可搬型メディアとしてフロッピーディスクやＰＤ、ＣＤ－ＲＯＭなどの他のメディアや、書換え可能型のＤＶＤを用い、メディア活用情報の記録領域については、メディア本体の記録領域を用いることも可能である。

【０１２２】なお、本実施の形態において、ＤＶＤの再生による使用量の算出について詳しく述べなかったが、ＤＶＤ再生装置１３００側で行う場合は、再生されたメディアの使用量を計算する手段を更に設け、再生（該メディアの使用）が終了したら、その使用量を使用量管理サーバ１３２０へ送信し、新たに使用量累計１５０４を更新し、一方、使用量管理サーバ１３２０側で行う場合は、タイトル情報の発行番号の通知を受けた時点で、任意の基準のもと、一定の使用量を加算するなどの方法が考えられる。

【０１２３】また、請求項１０に記載の発明のように、発行番号情報より更に階層的に使用量を管理する場合、つまり、例えば映画作品ＤＶＤの中に複数の映画作品が記録されている場合に、使用量累計を映画作品ごとに計算することも可能である。その場合には、利用者情報のエントリとしては、タイトル情報と発行番号情報とともにＤＶＤ内の映画作品を区別する情報で使用量累計を管理し、ＤＶＤ再生装置からＤＶＤの使用を通知する場合にも、ＤＶＤ内の映画作品を区別する情報をともに使用量管理サーバに送信することになる。図１７は、映画作品を区別する情報として映画作品名を用いた場合の利用者情報の構成例である。１７００は利用者情報、１７０１は前記メディア活用情報１４００内に含まれるタイトル情報、１７０２は前記メディア活用情報１４００内に含まれる発行番号情報、１７０７は映画作品名、１７０４は前記タイトル情報１７０１と前記発行番号情報１７０２と前記映画作品名１７０７とによって特定可能な可搬型メディア内の映画作品の使用量の累計を示す、使用量累計である。ここで、図１７においては、一つのエントリのみ示したが、実際には、このような形式で複数のエントリが存在する。

【０１２４】また、本実施の形態においては特に述べなかったが、使用量累計に加算される量は、タイトル情報、あるいは複数の映画作品が記録されている場合には、映画作品ごとに異なっても良く、その場合には、映画作品ＤＶＤを管理するためのＤＶＤ情報を設けて、加算すべき使用量を管理しておくという形態も考えられる。

【０１２５】以上のように、本実施の形態では、可搬型メディアの使用量を管理することにより、使用量に応じた課金を行うことができるとともに、その使用量をもとにユーザの利用状況（市場動向）を分析し、その分析結果を利用してユーザのより細かい要望への対応ができるなど、その実用的効果は大きい。

【０１２６】（実施の形態５）次に、請求項１１又は１２に対応する第５の実施の形態について説明する．請求項１１に記載の発明のように、第４の実施の形態において、使用量の上限として、最大使用量があらかじめ決められており、利用者情報に記録されている場合には、こ

の最大使用量を超えないかどうかを使用量管理サーバで管理し、超える場合には、その旨をＤＶＤ再生装置に通知して、再生できないようにするといった形態も考えられる。これについては、図１８に、使用量管理サーバで管理している利用者情報の構成例を示し、図１９に、最大使用量による管理を行う場合のフローチャートを示す。

【０１２７】以下、簡単に図１８と図１９について説明をする．図１８は、前述の形態に対して、更に最大使用量による管理を加えた場合の利用者情報の構成例である。図１８において、１８００は利用者情報、１８０１は前記メディア活用情報１４００内に含まれるタイトル情報、１８０２は前記メディア活用情報１４００内に含まれる発行番号情報、１８０４は前記タイトル情報１８０１と前記発行番号情報１８０２によって特定可能な可搬型メディアの使用量の累計を示す、使用量累計、１８０５は、この利用者情報１８００に設定されている最大使用量であって、可搬型メディアごとに異なっていてもよいものである。ここで、図１８においては、一つのエントリのみ示したが、実際には、このような形式で複数のエントリが存在する。これらは前記利用者情報管理手段１３３４によって管理されている。

【０１２８】図１９は図１８と同様、前述の形態に対して、更に最大使用量による管理を加えた場合の処理の流れを示すフローチャートである。図１９において、開始１９００、ステップ１９０１はそれぞれ図１６で示した開始１６００、ステップ１６０１と同じであるので説明を省略する。

【０１２９】次に、ステップ１９０２に示すように、使用量管理サーバ１３２０の中央制御手段１３２１は、情報送受信手段１３２４によりタイトル情報１４０１と発行番号情報１４０２とを受信し、利用者情報管理手段１３３４に対して、タイトル情報１４０１と発行番号情報１４０２とで管理されている利用者情報の使用量累計が最大使用量を超えていないかどうかを判断するように指示し、判断１９０３に進む。

【０１３０】次に、判断１９０３に示すように、利用者情報管理手段１３３４は、利用者情報を参照し、タイトル情報１４０１で発行番号情報１４０２の利用者情報のエントリを得て、その使用量累計１８０４が最大使用量１８０５を超えているかどうかを判断する。超えていない場合にはステップ１９０４に進み、超えている場合にはステップ１９０６に進む。

【０１３１】ステップ１９０４に進んだ場合には、利用者情報管理手段１３３４は、利用者情報１８００の使用量累計１８０４に対して、新たに今回の使用量を加算し、加算された結果の使用量累計１８０４を情報送受信手段１３２４により、ネットワーク１３４０を経由して、ＤＶＤ再生装置１３００に送信し、ステップ１９０５に示すように、ＤＶＤ再生装置１３００の中央制御手段１３０１は、使用量累計１８０４を情報送受信手段１３０４により受信し、情報表示手段１３０３にこれを表示したうえで、映画作品ＤＶＤ１３０６の再生を開始し、終了１９０８に進む。

【０１３２】一方、ステップ１９０６に進んだ場合には、使用量管理サーバ１３２０は、最大使用量を超えていることを情報送受信手段１３２４により、ネットワーク１３４０を経由して、ＤＶＤ再生装置１３００に送信し、ステップ１９０７に示すように、ＤＶＤ再生装置１３００の中央制御手段１３０１は、最大使用量を超えていることを情報送受信手段１３０４により受信し、情報表示手段１３０３にこれを表示し、終了１９０８に進む。

【０１３３】次に、請求項１２に記載の発明のように、第４の実施の形態において、使用量の上限としての最大使用量がメディア活用情報記録領域に記録されており、初回の利用時に使用量管理サーバに対して、この最大使用量を登録するといった形態も考えられる。これについては、図２０に、最大使用量が記録されている場合のメディア活用情報の構成例を示し、図２１に、最大使用量を登録する場合のフローチャートを示す。

【０１３４】以下、簡単に図２０と図２１について説明をする．図２０は、第４の実施の形態において、最大使用量をメディア活用情報にあらかじめ記録しておいた場合の、メディア活用情報の構成例である。図２０において、２０００はメディア活用情報、メディア活用情報２０００のうち、２００１は映画作品ＤＶＤの種類を特定可能なタイトル情報、２００２は該映画作品ＤＶＤを他のものと識別可能な、前記タイトル情報ごとの発行番号情報、２００５は該映画作品ＤＶＤを入手した際に設定されている最大使用量であり、映画作品ＤＶＤ配布時には既に前記メディア活用情報記録領域に記録済みである。

【０１３５】図２１は第４の実施の形態に対して、最大使用量をメディア活用情報にあらかじめ記録しておいた場合の処理の流れを示すフローチャートである。なお、図２１のフローチャートの説明においては、前記図１８で示した利用者情報も用いる。開始２１００は、図１６で示した開始１６００と同じであるので説明を省略する。

【０１３６】次に、ステップ２１０１に示すように、ＤＶＤ再生装置１３００の中央制御手段１３０１は映画作品ＤＶＤ１３０６の再生開始の指示を受け付け、ＤＶＤ駆動手段１３０７によって映画作品ＤＶＤ１３０６のメディア活用情報２０００のうちタイトル情報２００１と発行番号情報２００２と最大使用量２００５とを得て、タイトル情報２００１と発行番号情報２００２と最大使用量２００５とを情報送受信手段１３０４により、ネットワーク１３４０を経由して、使用量管理サーバ１３２０に対して送信し、ステップ２１０２に進む。

【０１３７】次に、ステップ２１０２に示すように、使用量管理サーバ１３２０の中央制御手段１３２１は、情報送受信手段１３２４によりタイトル情報２００１と発行番号情報２００２と最大使用量２００５とを受信し、利用者情報管理手段１３３４に対して、タイトル情報２００１と発行番号情報２００２とで管理されている利用者情報のエントリが既に登録されているかどうかを判断するように指示し、判断２１０３に進む。

【０１３８】次に、判断２１０３に示すように、利用者情報管理手段１３３４は、利用者情報を参照し、タイトル情報２００１で発行番号情報２００２の利用者情報のエントリを探し、既に登録されている場合には、利用者情報１８００としてステップ２１０５に進み、登録されていない場合には、ステップ２１０４に進む。

【０１３９】ステップ２１０４に進んだ場合には、利用者情報管理手段１３３４は、タイトル情報２００１で発行番号情報２００２の利用者情報１８００を新たに作成し、１８０１としてタイトル情報２００１、１８０２として発行番号情報２００２、１８０５として最大使用量２００５を設定し、ステップ２１０５に進む。

【０１４０】次に、ステップ２１０５に示すように、利用者情報管理手段１３３４は、利用者情報１８００の使用量累計１８０４に対して、新たに今回の使用量を加算し、加算された結果の使用量累計１８０４を情報送受信手段１３２４により、ネットワーク１３４０を経由して、ＤＶＤ再生装置１３００に送信し、ステップ２１０６に進む。

【０１４１】ステップ２１０６と終了２１０７は、それぞれ、図１６で示したステップ１６０６と終了１６０７と同じであるので説明を省略する。

【０１４２】以上のように、本実施の形態では、該可搬型メディアの使用量をもとに利用料金を利用者に対して請求したり、また、あらかじめ利用料金を払い込んである場合に、それに応じた最大使用量を超える場合にはその旨通知したりといったことが可能であって、可搬型メディアの無制限な利用を防止でき、その実用的効果は大きい。

【０１４３】（実施の形態６）次に、請求項１３に対応する第６の実施の形態について説明する．図２２は、本実施の形態における、可搬型メディアとして暗号化された映画作品を記録した、視聴の都度、視聴のための可搬型メディアの使用量の記録を行ない、使用量が最大使用量を超えない場合にのみ、鍵管理サーバから、復号用のデータ暗号化鍵を得ることが可能であるような、映画作品再生システムの構成を示す図である。

【０１４４】図２２において、２２００はＤＶＤ再生装置である。２２０１は前記ＤＶＤ再生装置２２００の動作全体を制御する中央制御手段、２２０２は前記ＤＶＤ再生装置２２００に対して利用者が入力を行なうキーボードやマウス、音声認識装置、タブレット、ペン、ボタン、リモートコントロールボタンなどの入力手段、２２０３は利用者に対して前記ＤＶＤ再生装置２２００が表示を行なうためのディスプレイ、スピーカなどの情報表示手段、２２０４は前記ＤＶＤ再生装置２２００のネットワークに対する情報の送受信を行なう情報送受信手段である。２２０６は映画作品をデータ暗号化鍵Ｄで暗号化して記録した映画作品ＤＶＤであって、そのメディア活用情報記録領域には、映画作品ＤＶＤの種類を特定可能なタイトル情報と、タイトル情報ごとの発行番号情報が記録されている。２２０７は前記映画作品ＤＶＤ２２０６を駆動するＤＶＤ駆動手段である。２２０８は前記データ暗号化鍵Ｄを用いて前記映画作品ＤＶＤ２２０６内の暗号化された映画作品を復号化するＤＶＤ内データ復号化手段である。２２０９は公開鍵暗号方式における、前記利用者の公開鍵に対応する利用者の秘密鍵が記録されているＩＣカード、２２１０は前記ＩＣカード２２０９を駆動するＩＣカード駆動手段である。２２１１は前記利用者の秘密鍵を用いて、前記暗号化データ暗号化鍵を復号化してデータ暗号化鍵Ｄを生成するデータ暗号化鍵復号化手段である。

【０１４５】２２２０は映画作品ＤＶＤ２２０６に記録されている映画作品の視聴のための可搬型メディアの使用量を記録し、かつ、データ暗号化鍵の管理を行なう鍵管理サーバである。２２２１は前記鍵管理サーバ２２２０の動作全体を制御する中央制御手段、２２２４は前記鍵管理サーバ２２２０のネットワークに対する情報の送受信を行なう情報送受信手段、２２３２は利用者に対して送信するデータ暗号化鍵を公開鍵暗号方式における利用者の公開鍵で暗号化する送信データ暗号化手段、２２３３は前記送信データ暗号化手段２２３２において利用する乱数を発生させる乱数発生手段、２２３４は映画作品ＤＶＤを再生する場合の可搬型メディアの使用量の累計と、最大使用量と、利用者の公開鍵とを前記タイトル情報と前記発行番号情報とによって管理する利用者情報管理手段、２２３５は前記データ暗号化鍵を前記タイトル情報によって管理するＤＶＤ情報管理手段である。２２４０は前記ＤＶＤ再生装置２２００と前記鍵管理サーバ２２２０との間を繋ぐネットワークである。

【０１４６】図２３は、本実施の形態にかかわるメディア活用情報の構成例である。図２３において、２３００はメディア活用情報、メディア活用情報２３００のうち、２３０１は映画作品ＤＶＤの種類を特定可能なタイトル情報、２３０２は該映画作品ＤＶＤを他のものと識別可能な、前記タイトル情報ごとの発行番号情報であり、映画作品ＤＶＤ配布時には既に前記メディア活用情報記録領域に記録済みである。

【０１４７】図２４は、本実施の形態にかかわる利用者情報の構成例である。図２４において、２４００は利用者情報、２４０１は前記メディア活用情報２３００内に含まれるタイトル情報、２４０２は前記メディア活用情

報２３００内に含まれる発行番号情報、２４０３は前記タイトル情報２４０１と前記発行番号情報２４０２とで特定可能な映画作品ＤＶＤを保有している利用者の、公開鍵暗号方式における公開鍵を含む利用者公開鍵情報、２４０４は前記タイトル情報２４０１と前記発行番号情報２４０２によって特定可能な可搬型メディアの使用量の累計を示す、使用量累計、２４０５は、この利用者情報２４００に設定されている最大使用量であって、可搬型メディアごとに異なっていてもよいものである。ここで、図２４においては、一つのエントリのみ示したが、実際には、このような形式で複数のエントリが存在する。これらは前記利用者情報管理手段２２３４によって管理されている。

【０１４８】図２５は、本実施の形態にかかわるＤＶＤ情報の構成例である。図２５において、２５００はＤＶＤ情報、２５０１は前記メディア活用情報２３００内にふくまれるタイトル情報、２５０２はこのタイトル情報２５０１によって特定可能な種類の映画作品ＤＶＤ内に記録されている映画作品を暗号化するのに用いたデータ暗号化鍵Ｄを含むデータ暗号化鍵情報である。ここで、図２５においては、一つのエントリのみ示したが、実際には、このような形式で複数のエントリが存在する。これらは前記ＤＶＤ情報管理手段２２３５によって管理されている。

【０１４９】図２６は本実施の形態の処理の流れを示すフローチャートである．以下、図２２から図２６を用いて本実施の形態の動作を説明する．利用者は書店や通信販売で購入、あるいは会員制のサービスによって配布してもらうことにより映画作品ＤＶＤ２２０６を入手する。

【０１５０】以降、利用者が映画作品ＤＶＤを再生する場合の、使用量の管理と、最大使用量を超えない場合のデータ暗号化鍵の取得を安全に行なう方法について、図２６のフローチャートに沿って説明する。なお、図２６においては角の丸い長方形で囲われた部分は、フローチャートの開始・終了を示し、長方形で囲われた部分は処理を示し、菱形で囲われた部分は判断を示し、矢印は処理の流れを示している。

【０１５１】まず、利用者は、映画作品ＤＶＤ２２０６をＤＶＤ再生装置２２００のＤＶＤ駆動手段２２０７にセットし、入力手段２２０２を用いて、再生開始をＤＶＤ再生装置２２００の中央制御手段２２０１に指示する。これにより、開始２６００に示すように、映画作品ＤＶＤの再生処理が開始される。

【０１５２】次に、ステップ２６０１に示すように、ＤＶＤ再生装置２２００の中央制御手段２２０１は映画作品ＤＶＤ２２０６の再生開始の指示を受け付け、ＤＶＤ駆動手段２２０７によって映画作品ＤＶＤ２２０６のメディア活用情報２３００のうちタイトル情報２３０１と発行番号情報２３０２とを得て、タイトル情報２３０１と発行番号情報２３０２とを情報送受信手段２２０４により、ネットワーク２２４０を経由して、鍵管理サーバ２２２０に対して送信し、映画作品ＤＶＤ２２０６に記録されているデータの復号化のためのデータ暗号化鍵の取得を依頼し、ステップ２６０２に進む。

【０１５３】次に、ステップ２６０２に示すように、鍵管理サーバ２２２０の中央制御手段２２２１は、情報送受信手段２２２４によりタイトル情報２３０１と発行番号情報２３０２とを受信し、利用者情報管理手段２２３４に対して、タイトル情報２３０１と発行番号情報２３０２とで管理されている利用者情報の映画作品ＤＶＤの使用量累計が最大使用量を超えているかどうかを判断させる指示を行ない、判断２６０３に進む。

【０１５４】次に、判断２６０３に示すように、利用者情報管理手段２２３４は、利用者情報を参照し、タイトル情報２３０１で発行番号情報２３０２の利用者情報のエントリ２４００を得て、その使用量累計２４０４が最大使用量２４０５を超えているかどうかを判断する。超えていない場合にはステップ２６０４に進み、超えている場合にはステップ２６１０に進む。ここで、利用者情報２４００のうちのタイトル情報２４０１と発行番号情報２４０２とは、それぞれ前記タイトル情報２３０１と前記発行番号情報２３０２とに等しい。

【０１５５】ここで、ステップ２６０４に進んだ場合には、利用者情報管理手段２２３４は、利用者情報２４００の使用量累計２４０４に対して、新たに今回の使用量を加算し、ＤＶＤ情報管理手段２２３５において、タイトル情報２３０１を元に、データ暗号化鍵情報２５０２を得て、ステップ２６０５に進む。ここで、ＤＶＤ情報２５００のうちのタイトル情報２５０１は、前記タイトル情報２３０１と等しい。

【０１５６】次に、ステップ２６０５に示すように、利用者情報管理手段２２３４によって、タイトル情報２３０１と発行番号情報２３０２とを元に、利用者公開鍵情報２４０３を得て、ステップ２６０６に進む。

【０１５７】次に、ステップ２６０６に示すように、乱数発生手段２２３３により、乱数Ｒを発生させ、ステップ２６０７に進む。

【０１５８】次に、ステップ２６０７に示すように、送信データ暗号化手段２２３２において、前記乱数Ｒを用いて、前記データ暗号化鍵情報２５０２に含まれているデータ暗号化鍵Ｄを暗号化し、さらに、Ｒと前記暗号化されたＤとを組合せたデータを、利用者情報管理手段２２３４によって得られる利用者公開鍵情報２４０３に含まれている利用者公開鍵ＰＵによって暗号化し、その結果を、情報送受信手段２２２４により、ネットワーク２２４０を経由してＤＶＤ再生装置２２００に送信し、ステップ２６０８に進む。

【０１５９】次に、ステップ２６０８に示すように、ＤＶＤ再生装置２２００は情報送受信手段２２０４により

鍵管理サーバ２２２０からの暗号化されたデータを受信し、さらに、中央制御手段２２０１の指示に従い、ＩＣカード駆動手段２２１０は、ＩＣカード２２０９に格納されている利用者秘密鍵ＳＵを得て、データ暗号化鍵復号化手段２２１１により、データ暗号化鍵Ｄを得て、ステップ２６０９に進む。

【０１６０】次に、ステップ２６０９に示すように、ＤＶＤ内データ復号化手段２２０８はステップ２６０８で得たデータ暗号化鍵Ｄを用いて、映画作品ＤＶＤ２２０６上の暗号化されているデータを復号化し、情報表示手段２２０３によって利用者に表示し、終了２６１２へ進む。

【０１６１】一方、判断２６０３からステップ２６１０に進んだ場合には、鍵管理サーバ２２２０は、最大使用量を超えていることを情報送受信手段２２２４により、ネットワーク２２４０を経由して、ＤＶＤ再生装置２２００に送信し、ステップ２６１１に進む。

【０１６２】次に、ステップ２６１１に示すように、ＤＶＤ再生装置２２００の中央制御手段２２０１は、最大使用量を超えていることを情報送受信手段２２０４により受信し、情報表示手段２２０３にこれを表示し、終了２６１２へ進む。

【０１６３】なお、本実施の形態においては可搬型メディアとしてＤＶＤ、メディア活用情報の記録領域としてＤＶＤ上のメディア活用情報記録領域を用いたが、可搬型メディアとしてフロッピーディスクやＰＤ、ＣＤ－ＲＯＭなどの他のメディアや、書換え可能型のＤＶＤを用い、メディア活用情報の記録領域については、メディア本体の記録領域を用いることも可能である。

【０１６４】以上のように、本実施の形態では、該可搬型メディアの使用量を記録することが可能であるため、あらかじめ利用者から徴収した料金に見合う最大使用量を設定しておき、使用量累計が最大使用量に達っするまでは利用者の要求に応じてデータ暗号化鍵を渡して、可搬型メディアの使用の可否を制御することにより、可搬型メディアの無制限な利用を確実に防止でき、その実用的効果は大きい。

【０１６５】（実施の形態７）次に、請求項１３に記載の発明に請求項１４に記載の発明を結合させた第７の実施の形態について説明する。

【０１６６】図２７は、本実施の形態による、可搬型メディアとして暗号化された映画作品を記録した、視聴の都度、視聴のための可搬型メディアの使用量の記録を行ない、使用量が最大使用量を超えない場合にのみ、鍵管理サーバから、復号用のデータ暗号化鍵を得ることが可能であって、かつ、鍵管理サーバに対しては、データを暗号化して送信するような、映画作品再生システムの構成を示す図である。

【０１６７】図２７において、２７００はＤＶＤ再生装置である。２７０１は前記ＤＶＤ再生装置２７００の動作全体を制御する中央制御手段、２７０２は前記ＤＶＤ再生装置２７００に対して利用者が入力を行なうキーボードやマウス、音声認識装置、タブレット、ペン、ボタン、リモートコントロールボタンなどの入力手段、２７０３は利用者に対して前記ＤＶＤ再生装置２７００が表示を行なうためのディスプレイ、スピーカなどの情報表示手段、２７０４は前記ＤＶＤ再生装置２７００のネットワークに対する情報の送受信を行なう情報送受信手段、２７０５は前記情報送受信手段２７０４などから得られる情報を一時的に記憶しておく情報記憶手段である。２７０６は映画作品をデータ暗号化鍵Ｄで暗号化して記録した映画作品ＤＶＤであって、そのメディア活用情報記録領域には、映画作品ＤＶＤの種類を特定可能なタイトル情報と、タイトル情報ごとの発行番号情報、公開鍵暗号方式における利用者の公開鍵が記録されている。２７０７は前記映画作品ＤＶＤ２７０６を駆動するＤＶＤ駆動手段である。２７０８は前記データ暗号化鍵Ｄを用いて前記映画作品ＤＶＤ２７０６内の暗号化された映画作品を復号化するＤＶＤ内データ復号化手段ある。２７０９は公開鍵暗号方式における、前記利用者の公開鍵に対応する利用者の秘密鍵が記録されているＩＣカード、２７１０は前記ＩＣカード２７０９を駆動するＩＣカード駆動手段である。２７１１は前記利用者の秘密鍵を用いて、前記暗号化データ暗号化鍵を復号化してデータ暗号化鍵Ｄを生成するデータ暗号化鍵復号化手段、２７１２は鍵管理サーバにデータを送信する際に、鍵管理サーバの公開鍵を用いてデータを暗号化し、暗号化データとする、送信データ暗号化手段である。

【０１６８】２７２０は映画作品ＤＶＤ２７０６に記録されている映画作品の視聴のための可搬型メディアの使用量を記録し、かつ、データ暗号化鍵の管理を行なう鍵管理サーバである。２７２１は前記鍵管理サーバ２７２０の動作全体を制御する中央制御手段、２７２４は前記鍵管理サーバ２７２０のネットワークに対する情報の送受信を行なう情報送受信手段、２７２５は前記情報送受信手段２７２４から得られる情報や、鍵管理サーバ２７２０自身で生成した情報を一時的に記憶しておく情報記憶手段である。２７２９は公開鍵暗号方式における、前記鍵管理サーバの公開鍵に対応する鍵管理サーバの秘密鍵が記録されているＩＣカード、２７３０は前記ＩＣカード２７２９を駆動するＩＣカード駆動手段である。２７３１は前記鍵管理サーバの秘密鍵を用いて、前記ＤＶＤ再生装置２７００から送信されてきた暗号化データを復号化する受信データ復号化手段である。２７３２は利用者に対して送信するデータ暗号化鍵を公開鍵暗号方式における利用者の公開鍵で暗号化する送信データ暗号化手段、２７３３は前記送信データ暗号化手段２７１２と、前記送信データ暗号化手段２７３２とにおいて利用する乱数を発生させる乱数発生手段、２７３４は映画作品ＤＶＤを再生する場合の可搬型メディアの使用量の累

計と、最大使用量と、利用者の公開鍵とを前記タイトル情報と前記発行番号情報とによって管理する利用者情報管理手段、２７３５は前記データ暗号化鍵を前記タイトル情報によって管理するＤＶＤ情報管理手段である。２７４０は前記ＤＶＤ再生装置２７００と前記鍵管理サーバ２７２０との間を繋ぐネットワークである。

【０１６９】図２８は、本実施の形態にかかわるメディア活用情報の構成例である．図２８において、２８００はメディア活用情報、メディア活用情報２８００のうち、２８０１は映画作品ＤＶＤの種類を特定可能なタイトル情報、２８０２は該映画作品ＤＶＤを他のものと識別可能な、前記タイトル情報ごとの発行番号情報、２８０４は鍵管理サーバの、公開鍵暗号方式における公開鍵を含む、鍵管理サーバ公開鍵情報であり、映画作品ＤＶＤ配布時には既に前記メディア活用情報記録領域に記録済みである。

【０１７０】図２９は、本実施の形態にかかわる利用者情報の構成例である．図２９において、２９００は利用者情報、２９０１は前記メディア活用情報２８００内に含まれるタイトル情報、２９０２は前記メディア活用情報２８００内に含まれる発行番号情報、２９０３は前記タイトル情報２９０１と前記発行番号情報２９０２とで特定可能な映画作品ＤＶＤを保有している利用者の、公開鍵暗号方式における公開鍵を含む利用者公開鍵情報、２９０４は前記タイトル情報２９０１と前記発行番号情報２９０２によって特定可能な可搬型メディアの使用量の累計を示す、使用量累計、２９０５は、この利用者情報２９００に設定されている最大使用量であって、可搬型メディアごとに異なっていてもよいものである。ここで、図２９においては、一つのエントリのみ示したが、実際には、このような形式で複数のエントリが存在する。これらは前記利用者情報管理手段２７３４によって管理されている。

【０１７１】図３０は、本実施の形態にかかわるＤＶＤ情報の構成例である．図３０において、３０００はＤＶＤ情報、３００１は前記メディア活用情報２８００内に含まれるタイトル情報、３００２はこのタイトル情報３００１によって特定可能な種類の映画作品ＤＶＤ内に記録されている映画作品を暗号化するのに用いたデータ暗号化鍵Ｄを含むデータ暗号化鍵情報である。ここで、図３０においては、一つのエントリのみ示したが、実際には、このような形式で複数のエントリが存在する。これらは前記ＤＶＤ情報管理手段２７３５によって管理されている。

【０１７２】図３１は、本実施の形態の処理の流れを示すフローチャートである．以下、図２７から図３１を用いて本実施の形態の動作を説明する．利用者は書店や通信販売で購入、あるいは会員制のサービスによって配布してもらうことにより映画作品ＤＶＤ２７０６を入手する。

【０１７３】以降、利用者が映画作品ＤＶＤを再生する場合の、使用量の管理と、最大使用量を超えない場合のデータ暗号化鍵の取得と取得の以来とを安全に行なう方法について、図３１のフローチャートに沿って説明する。なお、図３１においては角の丸い長方形で囲われた部分は、フローチャートの開始・終了を示し、長方形で囲われた部分は処理を示し、菱形で囲われた部分は判断を示し、矢印は処理の流れを示している。

【０１７４】まず、利用者は、映画作品ＤＶＤ２７０６をＤＶＤ再生装置２７００のＤＶＤ駆動手段２７０７にセットし、入力手段２７０２を用いて、再生開始をＤＶＤ再生装置２７００の中央制御手段２７０１に指示する。これにより、開始３１００に示すように、映画作品ＤＶＤの再生処理が開始される。

【０１７５】次に、ステップ３１０１に示すように、ＤＶＤ再生装置２７００の中央制御手段２７０１は、情報送受信手段２７０４により、ネットワーク２７４０を経由して、鍵管理サーバ２７２０に対して、まず乱数の取得を依頼し、ステップ３１０２に進む。

【０１７６】次に、ステップ３１０２に示すように、鍵管理サーバ２７２０の中央制御手段２７２１は、乱数取得依頼の指示を、情報送受信手段２７２４により受信し、乱数発生手段２７３３により乱数Ｒを発生させ、情報記憶手段２７２５に乱数Ｒを記憶させ、乱数Ｒを、情報送受信手段２７２４により、ネットワーク２７４０を経由して、ＤＶＤ再生装置２７００に送信し、ステップ３１０３に進む。

【０１７７】次に、ステップ３１０３に示すように、ＤＶＤ再生装置２７００の中央制御手段２７０１は、乱数Ｒを情報送受信手段２７０４により受信し、乱数Ｒは情報記憶手段２７０５に記憶させ、送信データ暗号化手段２７１２は、情報記憶手段２７０５に記憶させておいた乱数Ｒと、ＤＶＤ駆動手段２７０７によって映画作品ＤＶＤ２７０６のメディア活用情報２８００から得られる鍵管理サーバ公開鍵情報２８０４に含まれている鍵管理サーバ公開鍵ＰＳとを用いて、同じく映画作品ＤＶＤ２７０６のメディア活用情報２８００から得られるタイトル情報２８０１と発行番号情報２８０２とを暗号化し、ステップ３１０４に進む。

【０１７８】次に、ステップ３１０４に示すように、ＤＶＤ再生装置２７００の中央制御手段２７０１の指示により、情報送受信手段２７０４は、ネットワーク２７４０を経由して、鍵管理サーバ２７２０に対して、暗号化されたタイトル情報２８０１と発行番号情報２８０２とを送信し、データ暗号化鍵の取得を鍵管理サーバ２７２０に依頼し、ステップ３１０５に進む。

【０１７９】次に、ステップ３１０５に示すように、鍵管理サーバ２７２０は情報送受信手段２７２４によりＤＶＤ再生装置２７００からの暗号化されたデータを受信し、さらに、中央制御手段２７２１の指示に従い、ＩＣ

カード駆動手段２７３０は、ＩＣカード２７２９に格納されている鍵管理サーバ秘密鍵ＳＳを得て、受信データ復号化手段２７３１により、タイトル情報２８０１と発行番号情報２８０２とを復号化し、判断３１０６に進む。

【０１８０】次に、判断３１０６に示すように、ステップ３１０５において、送信されたデータから得られた乱数Ｒが情報記憶手段２７２５に記憶してある乱数と等しいかどうかを判断し、等しい場合には、Ｒを用いて正しく復号化できたものとしてステップ３１０７に進み、等しくない場合には正しく復号化できなかったものとしてステップ３１１２に進む。

【０１８１】ステップ３１０７に進んだ場合には、鍵管理サーバ２７２０の中央制御手段２７２１は、ステップ３１０５で得たタイトル情報２８０１と発行番号情報２８０２とを用いて、利用者情報管理手段２７３４に対して、タイトル情報２８０１と発行番号情報２８０２とで管理されている利用者情報の映画作品ＤＶＤの使用量累計が最大使用量を超えているかどうかを判断させる指示を行ない、判断３１０８に進む。

【０１８２】次に、判断３１０８に示すように、利用者情報管理手段２７３４は、利用者情報を参照し、タイトル情報２８０１で発行番号情報２８０２の利用者情報のエントリ２９００を得て、その使用量累計２９０４が最大使用量２９０５を超えているかどうかを判断する。超えていない場合にはステップ３１０９に進み、超えている場合にはステップ３１１３に進む。ここで、利用者情報２９００のうちのタイトル情報２９０１と発行番号情報２９０２とは、それぞれ前記タイトル情報２８０１と前記発行番号情報２８０２とに等しい。

【０１８３】ステップ３１０９に進んだ場合には、ＤＶＤ情報管理手段２７３５は、タイトル情報２８０１を元に、ＤＶＤ情報３０００からデータ暗号化鍵情報３００２を得、利用者情報管理手段２７３４は、利用者情報２９００の使用量累計２９０４に対して、新たに今回の使用量を加算し、さらに、利用者公開鍵情報２９０３を得て、ステップ３１１０に進む。ここで、ＤＶＤ情報３０００のうちのタイトル情報３００１は、前記タイトル情報２８０１と等しい。

【０１８４】次に、ステップ３１１０に示すように、送信データ暗号化手段２７３２において、情報記憶手段２７２５に記憶してある乱数Ｒを用いて、前記データ暗号化鍵情報３００２に含まれているデータ暗号化鍵Ｄを暗号化し、さらに、Ｒと前記暗号化されたＤとを組合せたデータを、ステップ３１０９で得られた利用者公開鍵情報２９０３に含まれている利用者公開鍵ＰＵによって暗号化し、その結果を、情報送受信手段２７２４により、ネットワーク２７４０を経由してＤＶＤ再生装置２７００に送信し、ステップ３１１１に進む。

【０１８５】次に、ステップ３１１１に示すように、まず、ＤＶＤ再生装置２７００は情報送受信手段２７０４により鍵管理サーバ２７２０からの暗号化されたデータを受信し、さらに、中央制御手段２７０１の指示に従い、ＩＣカード駆動手段２７１０は、ＩＣカード２７０９に格納されている利用者秘密鍵ＳＵを得て、データ暗号化鍵復号化手段２７１１により、データ暗号化鍵Ｄを得る。この際、情報記憶手段２７０５に記憶しておいた乱数Ｒと、データ暗号化鍵復号化手段において得られる乱数とが等しいことを確認する。次に、ＤＶＤ内データ復号化手段２７０８において、データ暗号化鍵Ｄを用いて、映画作品ＤＶＤ２７０６上の暗号化されているデータを復号化し、情報表示手段２７０３によって利用者に表示し、終了３１１５へ進む。

【０１８６】また、判断３１０６からステップ３１１２に進んだ場合には、ネットワークの障害によってＲの値が正しく送信されなかったか、あるいは不正な利用者が介在したために、Ｒの値が正しく送信されなかったかのどちらかであとし、処理を中断する。

【０１８７】また、判断３１０８からステップ３１１３に進んだ場合には、鍵管理サーバ２７２０は、最大使用量を超えていることを情報送受信手段２７２４により、ネットワーク２７４０を経由して、ＤＶＤ再生装置２７００に送信し、ステップ３１１４に進む。

【０１８８】次に、ステップ３１１４に示すように、ＤＶＤ再生装置２７００の中央制御手段２７０１は、最大使用量を超えていることを情報送受信手段２７０４により受信し、情報表示手段２７０３にこれを表示し、終了３１１５へ進む。

【０１８９】なお、本実施の形態においては可搬型メディアとしてＤＶＤ、メディア活用情報の記録領域としてＤＶＤ上のメディア活用情報記録領域を用いたが、可搬型メディアとしてフロッピーディスクやＰＤ、ＣＤ－ＲＯＭなどの他のメディアや、着換え可能型のＤＶＤを用い、メディア活用情報の記録領域については、メディア本体の記録領域を用いることも可能である。

【０１９０】以上のように、本実施の形態では、該可搬型メディアの使用量を記録することが可能であるため、あらかじめ利用者から徴収した料金に見合う最大使用量を設定しておき、使用量累計が最大使用量に達っするまでは利用者の要求に応じてデータ暗号化鍵を渡して、可搬型メディアの使用の可否を制御することにより、可搬型メディアの無制限な利用を確実に防止するという効果を奏するもので、かつ、利用者の要求を鍵管理サーバに送信する場合には、タイトル情報や発行番号情報などの機密の情報が第三者に漏洩することのないように、暗号化して送信することで、安全なデータ転送をも可能とし、その実用的効果は大きい。

【０１９１】（実施の形態８）次に、請求項１５乃至１８に対応する第８の実施の形態について説明する．図３２は、本発明の第７の実施の形態による、可搬型メディ

アとして映画作品を記録した可搬型メディアに対して、視聴の都度、有効期限を有効期限管理サーバに確認後再生を行なう映画作品再生システムの構成を示す図である。図３２において、３２００はＤＶＤ再生装置である。３２０１は前記ＤＶＤ再生装置３２００の動作全体を制御する中央制御手段、３２０２は前記ＤＶＤ再生装置３２００に対して利用者が入力を行なうキーボードやマウス、音声認識装置、タブレット、ペン、ボタン、リモートコントロールボタンなどの入力手段、３２０３は利用者に対して前記ＤＶＤ再生装置３２００が表示を行なうためのディスプレイ、スピーカなどの情報表示手段、３２０４は前記ＤＶＤ再生装置３２００のネットワークに対する情報の送受信を行なう情報送受信手段である。３２０６は映画作品を記録した映画作品ＤＶＤであって、そのメディア活用情報記録領域には、映画作品ＤＶＤの種類を特定可能なタイトル情報と、タイトル情報ごとの発行番号情報とが記録されている。３２０７は前記映画作品ＤＶＤ３２０６を駆動するＤＶＤ駆動手段である。

【０１９２】３２２０は映画作品ＤＶＤ３２０６が使用有効期限内であるかどうかを判断する有効期限管理サーバである。３２２１は前記有効期限管理サーバ３２２０の動作全体を制御する中央制御手段、３２２４は前記有効期限管理管理サーバ３２２０のネットワークに対する情報の送受信を行なう情報送受信手段、３２３４は映画作品ＤＶＤ使用有効期限を前記タイトル情報と前記発行番号情報とによって管理する利用者情報管理手段、３２３６は現在時刻を発生させる現在時刻発生手段、３２３７は現在時刻発生手段３２３６によって得られた現在時刻と使用有効期限とを比較し、映画作品ＤＶＤが使用有効期限内であるかどうかを判断する使用有効期限判断手段である。３２４０は前記ＤＶＤ再生装置３２００と前記鍵管理サーバ３２２０との間を繋ぐネットワークである。

【０１９３】図３３は、本実施の形態にかかわるメディア活用情報の構成例である。図３３において、３３００はメディア活用情報、メディア活用情報３３００のうち、３３０１は映画作品ＤＶＤの種類を特定可能なタイトル情報、３３０２は該映画作品ＤＶＤを他のものと識別可能な、前記タイトル情報ごとの発行番号情報であり、映画作品ＤＶＤ配布時には既に前記メディア活用情報記録領域に記録済みである。

【０１９４】図３４は、本実施の形態にかかわる利用者情報の構成例である。図３４において、３４００は利用者情報、３４０１は前記メディア活用情報３３００内に含まれるタイトル情報、３４０２は前記メディア活用情報３３００内に含まれる発行番号情報、３４０６は前記タイトル情報３４０１と前記発行番号情報３４０２によって特定可能な可搬型メディアの使用有効期限を示す、使用有効期限情報であって、可搬型メディアごとに異なっていてもよいものである。ここで、図３４においては、一つのエントリのみ示したが、実際には、このような形式で複数のエントリが存在する。これらは前記利用者情報管理手段３２３４によって管理されている。

【０１９５】図３５は本実施の形態の処理の流れを示すフローチャートである。以下、図３２から図３５を用いて本実施の形態の動作を説明する。

【０１９６】利用者は書店や通信販売で購入、あるいは会員制のサービスによって配布してもらうことにより映画作品ＤＶＤ３２０６を入手する。

【０１９７】以降、利用者が映画作品ＤＶＤを再生する場合の、使用有効期限の管理について、図３５のフローチャートに沿って説明する。なお、図３５においては角の丸い長方形で囲われた部分は、フローチャートの開始・終了を示し、長方形で囲われた部分は処理を示し、菱形で囲われた部分は判断を示し、矢印は処理の流れを示している。

【０１９８】まず、利用者は、映画作品ＤＶＤ３２０６をＤＶＤ再生装置３２００のＤＶＤ駆動手段３２０７にセットし、入力手段３２０２を用いて、再生開始をＤＶＤ再生装置３２００の中央制御手段３２０１に指示する。これにより、開始３５００に示すように、映画作品ＤＶＤ３２０６の再生処理が開始される。

【０１９９】次に、ステップ３５０１に示すように、ＤＶＤ再生装置３２００の中央制御手段３２０１は映画作品ＤＶＤ３２０６の再生開始の指示を受け付け、ＤＶＤ駆動手段３２０７によって映画作品ＤＶＤ３２０６のメディア活用情報３３００のうちタイトル情報３３０１と発行番号情報３３０２とを得て、タイトル情報３３０１と発行番号情報３３０２とを情報送受信手段３２０４により、ネットワーク３２４０を経由して、有効期限管理サーバ３２２０に対して送信し、ステップ３５０２に進む。

【０２００】次に、ステップ３５０２に示すように、有効期限管理サーバ３２２０の中央制御手段３２２１は、情報送受信手段３２２４によりタイトル情報３３０１と発行番号情報３３０２とを受信し、利用者情報管理手段３２３４は、これを元に利用者情報３４００を得て、そのうちの使用有効期限情報３４０６を得て、ステップ３５０３に進む。ここで、３４０１は前記タイトル情報３３０１に等しく、３４０２は前記発行番号情報３３０２に等しい。

【０２０１】次に、ステップ３５０３に示すように、有効期限管理サーバ３２２０の中央制御手段３２２１は、現在時刻発生手段３２３６によって現在時刻Ｃを発生させ、判断３５０４に進む。

【０２０２】次に、判断３５０４に示すように、使用有効期限判断手段３２３７において、前記得られた使用有効期限情報３４０６に含まれている有効期限と現在時刻Ｃとを比較し、現在時刻Ｃが有効期限内であるかどうか

を判断し、有効期限内である場合にはステップ３５０５に進み、有効期間外である場合にはステップ３５０７に進む。

【０２０３】ステップ３５０５に進んだ場合は、有効期限管理サーバ３２２０の中央制御手段３２２１は、有効期限内である旨を情報送受信手段３２２４により、ネットワーク３２４０を経由して、ＤＶＤ再生装置３２００に送信し、ステップ３５０６に進む。

【０２０４】次に、ステップ３５０６に示すように、ＤＶＤ再生装置３２００の中央制御手段３２０１は、有効期限内である旨を情報送受信手段３２０４により受信し、情報表示手段３２０３にこれを表示したうえで、映画作品ＤＶＤ３２０６の再生を開始し、終了３５０９に進む。

【０２０５】また、ステップ３５０７に進んだ場合は、有効期限管理サーバ３２２０の中央制御手段３２２１は、有効期限外である旨を情報送受信手段３２２４により、ネットワーク３２４０を経由して、ＤＶＤ再生装置３２００に送信し、ステップ３５０８に進む。

【０２０６】次に、ステップ３５０８に示すように、ＤＶＤ再生装置３２００の中央制御手段３２０１は、有効期限外である旨を情報送受信手段３２０４により受信し、情報表示手段３２０３にこれを表示し、終了３５０９に進む。

【０２０７】また、本実施の形態においては特に述べなかったが、請求項１８に記載の発明のように、映画作品ＤＶＤの中に更に複数の映画作品が記録されている場合に、使用有効期限を映画作品ごとに設定することも可能である。その場合には、メディア活用情報に、映画作品ごとに使用有効期限情報を設定する形態、あるいは、利用者情報のエントリとして、タイトル情報と発行番号情報とともにＤＶＤ内の映画作品を区別する情報で使用有効期限を管理し、ＤＶＤ再生装置からＤＶＤの使用を通知する場合にも、ＤＶＤ内の映画作品を区別する情報をともに使用量管理サーバに送信することになる。

【０２０８】図３９は、映画作品を区別する情報として映画作品名を用いた場合の利用者情報の構成例である。３９００は利用者情報、３９０１は前記メディア活用情報３３００内に含まれるタイトル情報、３９０２は前記メディア活用情報３３００内に含まれる発行番号情報、３９０７は映画作品名、３９０６は前記タイトル情報３９０１と前記発行番号情報３９０２と前記映画作品名３９０７とによって特定可能な可搬型メディア内の映画作品の使用有効期限を示す、使用有効期限情報である。ここで、図３９においては、一つのエントリのみ示したが、実際には、このような形式で複数のエントリが存在する。

【０２０９】このように、本実施の形態では、可搬型メディアに対してあらかじめ使用有効期限を設定した場合に、それを超えて該可搬型メディアを利用しようとする場合にその旨通知したり、また、あらかじめ利用料金を払い込んである場合に、それに応じた利用期間を超える場合にはその旨通知したりといったことが可能であって、可搬型メディアの無制限な利用を防止するという効果を奏するものである。

【０２１０】（実施の形態９）次に、請求項１９乃至２２に対応する第９の実施の形態について説明する．本実施の形態は、第８の実施の形態と異なる点として、使用有効期限情報を有効期限管理サーバではなく、可搬型メディアのメディア活用情報にあらかじめ記録しておき、可搬型メディアの利用の都度、メディア活用情報内の使用有効期限情報を有効期限管理サーバに対して送信し、有効期限内であるかどうかの判断をさせるといった形態にある。図３６は、この場合の構成例を示したものであり、利用者情報管理手段がない点を除けば、図３２の構成と同じ構成である。

【０２１１】図３７は、この場合のメディア活用情報の構成例であって、３７００はメディア活用情報、メディア活用情報３７００のうち、３７０６は該映画作品ＤＶＤの使用有効期限を示した使用有効期限情報であり、映画作品ＤＶＤ配布時には既に前記メディア活用情報記録領域に記録済みである。

【０２１２】図３８は、この場合の処理の流れを示すフローチャートであり、図３５のフローチャートとの相違は、ステップ３８０１に示すように、ＤＶＤ再生装置３６００の中央制御手段３６０１が映画作品ＤＶＤ３６０６の再生開始の指示を受け付けた際に、ＤＶＤ駆動手段３６０７によって映画作品ＤＶＤ３６０６のメディア活用情報３７００のうち使用有効期限情報３７０６を得て、使用有効期限情報３７０６を情報送受信手段３６０４により、ネットワーク３６４０を経由して、有効期限管理サーバ３６２０に対して送信し、ステップ３８０２に進む点。

【０２１３】次に、ステップ３８０２に示すように、有効期限管理サーバ３６２０の中央制御手段３６２１は、情報送受信手段３６２４により使用有効期限情報３７０６を受信し、そこから有効期限を得る点であり、その後の、有効期限を使用有効期限判断手段における現在時刻との比較を行い、その結果をＤＶＤ再生装置３６００に送信し、終了するまでのステップ３８０３から終了３８０９までの動作は図３５のフローチャートに記載したステップ３５０３から終了３５０９までの動作と同じである。

【０２１４】また、本実施の形態においては特に述べなかったが、請求項２１に記載の発明のように、映画作品ＤＶＤの中に更に複数の映画作品が記録されている場合に、使用有効期限を映画作品ごとに設定することも可能である。

【０２１５】また、本実施の形態においては特に述べなかったが、請求項２２に記載の発明のように、可搬型メ

ディアの内容が暗号化されいる場合は、使用有効期限内であることが判明した後、実施の形態２と同様の処理を行うことによってメディアの再生が可能となる。

【０２１６】以上のように、本実施の形態においても、第８の実施の形態と同様の効果が得られることは言うまでもない。

【０２１７】（実施の形態１０）次に、請求項２３に対応する第１０の実施の形態について説明する．図４０は、本実施の形態における、可搬型メディアとして暗号化された映画作品を記録した、視聴の都度、鍵管理サーバに対して使用有効期限の確認を行ない、使用有効期限内である場合にのみ、鍵管理サーバから、復号用のデータ暗号化鍵を得ることが可能であるような、映画作品再生システムの構成を示す図である。

【０２１８】図４０において、４０００はＤＶＤ再生装置である。４００１は前記ＤＶＤ再生装置４０００の動作全体を制御する中央制御手段、４００２は前記ＤＶＤ再生装置４０００に対して利用者が入力を行なうキーボードやマウス、音声認識装置、タブレット、ペン、ボタン、リモートコントロールボタンなどの入力手段、４００３は利用者に対して前記ＤＶＤ再生装置４０００が表示を行なうためのディスプレイ、スピーカなどの情報表示手段、４００４は前記ＤＶＤ再生装置４０００のネットワークに対する情報の送受信を行なう情報送受信手段である。４００６は映画作品をデータ暗号化鍵Ｄで暗号化して記録した映画作品ＤＶＤ、そのメディア活用情報記録領域には、映画作品ＤＶＤの種類を特定可能なタイトル情報と、タイトル情報ごとの発行番号情報が記録されている。４００７は前記映画作品ＤＶＤ４００６を駆動するＤＶＤ駆動手段である。４００８は前記データ暗号化鍵Ｄを用いて前記映画作品ＤＶＤ４００６内の暗号化された映画作品を復号化するＤＶＤ内データ復号化手段である。４００９は公開鍵暗号方式における、前記利用者の公開鍵に対応する利用者の秘密鍵が記録されているＩＣカード、４０１０は前記ＩＣカード４００９を駆動するＩＣカード駆動手段である。４０１１は前記利用者の秘密鍵を用いて、前記暗号化データ暗号化鍵を復号化してデータ暗号化鍵Ｄを生成するデータ暗号化鍵復号化手段である。

【０２１９】４０２０は映画作品ＤＶＤ４００６に記録されている映画作品の鍵管理サーバである。４０２１は前記鍵管理サーバ４０２０の動作全体を制御する中央制御手段、４０２４は前記鍵管理サーバ４０２０のネットワークに対する情報の送受信を行なう情報送受信手段、４０３２は利用者に対して送信するデータ暗号化鍵を公開鍵暗号方式における利用者の公開鍵で暗号化する送信データ暗号化手段、４０３３は前記送信データ暗号化手段において利用する乱数を発生させる乱数発生手段、４０３４は映画作品ＤＶＤの使用有効期限情報と利用者の公開鍵とを前記タイトル情報と前記発行番号情報とによって管理する利用者情報管理手段、４０３５は前記データ暗号化鍵を前記タイトル情報によって管理するＤＶＤ情報管理手段、４０３６は現在時刻を発生させる現在時刻発生手段、４０３７は現在時刻発生手段４０３６によって得られた現在時刻と使用有効期限とを比較し、映画作品ＤＶＤが使用有効期限内であるかどうかを判断する使用有効期限判断手段である。４０４０は前記ＤＶＤ再生装置４０００と前記鍵管理サーバ４０２０との間を繋ぐネットワークである。

【０２２０】図４１は、本実施の形態にかかわるメディア活用情報の構成例である。図４１において、４１００はメディア活用情報、メディア活用情報４１００のうち、４１０１は映画作品ＤＶＤの種類を特定可能なタイトル情報、４１０２は該映画作品ＤＶＤを他のものと識別可能な、前記タイトル情報ごとの発行番号情報であり、映画作品ＤＶＤ配布時には既に前記メディア活用情報記録領域に記録済みである。

【０２２１】図４２は、本実施の形態にかかわる利用者情報の構成例である。図４２において、４２００は利用者情報、４２０１は前記メディア活用情報４１００内に含まれるタイトル情報、４２０２は前記メディア活用情報４１００内に含まれる発行番号情報、４２０３は前記タイトル情報４２０１と前記発行番号情報４２０２とで特定可能な映画作品ＤＶＤを保有している利用者の、公開鍵暗号方式における公開鍵を含む利用者公開鍵情報、４２０６は前記タイトル情報４２０１と前記発行番号情報４２０２によって特定可能な可搬型メディアの使用有効期限を示す、使用有効期限情報であって、可搬型メディアごとに異なっていてもよいものである。ここで、図４２においては、一つのエントリのみ示したが、実際には、このような形式で複数のエントリが存在する。これらは前記利用者情報管理手段４０３４によって管理されている。

【０２２２】図４３は、本実施の形態にかかわるＤＶＤ情報の構成例である。図４３において、４３００はＤＶＤ情報、４３０１は前記メディア活用情報４１００内にふくまれるタイトル情報、４３０２はこのタイトル情報４３０１によって特定可能な種類の映画作品ＤＶＤ内に記録されている映画作品を暗号化するのに用いたデータ暗号化鍵Ｄを含むデータ暗号化鍵情報である。ここで、図４３においては、一つのエントリのみ示したが、実際には、このような形式で複数のエントリが存在する。これらは前記ＤＶＤ情報管理手段４０３５によって管理されている。

【０２２３】図４４は本実施の形態の処理の流れを示すフローチャートである．以下、図４０から図４４を用いて本実施の形態の動作を説明する．利用者は書店や通信販売で購入、あるいは会員制のサービスによって配布してもらうことにより映画作品ＤＶＤ４００６を入手する。

【０２２４】以降、利用者が映画作品ＤＶＤを再生する場合の、使用有効期限の管理と、使用有効期限を超えない場合のデータ暗号化鍵の取得を安全に行なう方法について、図４４のフローチャートに沿って説明する。なお、図４４においては角の丸い長方形で囲われた部分は、フローチャートの開始・終了を示し、長方形で囲われた部分は処理を示し、菱形で囲われた部分は判断を示し、矢印は処理の流れを示している。

【０２２５】まず、利用者は、映画作品ＤＶＤ４００６をＤＶＤ再生装置４０００のＤＶＤ駆動手段４００７にセットし、入力手段４００２を用いて、再生開始をＤＶＤ再生装置４０００の中央制御手段４００１に指示する。これにより、開始４４００に示すように、映画作品ＤＶＤ４００６の再生処理が開始される。

【０２２６】次に、ステップ４４０１に示すように、ＤＶＤ再生装置４０００の中央制御手段４００１は映画作品ＤＶＤ４００６の再生開始の指示を受け付け、ＤＶＤ駆動手段４００７によって映画作品ＤＶＤ４００６のメディア活用情報４１００のうちタイトル情報４１０１と発行番号情報４１０２とを得て、タイトル情報４１０１と発行番号情報４１０２とを情報送受信手段４００４により、ネットワーク４０４０を経由して、鍵管理サーバ４０２０に対して送信し、映画作品ＤＶＤ４００６に記録されているデータの復号化のためのデータ暗号化鍵の取得を依頼し、ステップ４４０２に進む。

【０２２７】次に、ステップ４４０２に示すように、鍵管理サーバ４０２０の中央制御手段４０２１は、情報送受信手段４０２４によりタイトル情報４１０１と発行番号情報４１０２とを受信し、利用者情報管理手段４０３４に対して、タイトル情報４１０１と発行番号情報４１０２とで管理されている利用者情報のエントリ４２００を得て、その使用有効期限情報４２０６を得、また、現在時刻発生手段４０３６により、現在時刻Ｃを得て、判断４４０３に進む。ここで、利用者情報４２００のうちのタイトル情報４２０１と発行番号情報４２０２とは、それぞれ前記タイトル情報４１０１と発行番号情報４１０２とに等しい。

【０２２８】次に、判断４４０３に示すように、使用有効期限判断手段４０３７において、現在時刻Ｃが、前記得られた使用有効期限情報４２０６に含まれている有効期限内であるかどうかを判断し、有効期限内である場合には、ステップ４４０４に進み、有効期限外である場合には、ステップ４４１０に進む。

【０２２９】ステップ４４０４に進んだ場合には、ＤＶＤ情報管理手段４０３５は、タイトル情報４１０１を元に、データ暗号化鍵情報４３０２を得て、ステップ４４０５に進む。ここで、ＤＶＤ情報４３００のうちのタイトル情報４３０１は、前記タイトル情報４１０１と等しい。

【０２３０】次に、ステップ４４０５に示すように、利用者情報管理手段４０３４によって、タイトル情報４１０１と発行番号情報４１０２とを元に、利用者公開鍵情報４２０３を得て、ステップ４４０６に進む。

【０２３１】次に、ステップ４４０６に示すように、乱数発生手段４０３３により、乱数Ｒを発生させ、ステップ４４０７に進む。

【０２３２】次に、ステップ４４０７に示すように、送信データ暗号化手段４０３２において、前記乱数Ｒを用いて、前記データ暗号化鍵情報４３０２に含まれているデータ暗号化鍵Ｄを暗号化し、さらに、Ｒと前記暗号化されたＤとを組合せたデータを、利用者情報管理手段４０３４によって得られる利用者公開鍵情報４２０３に含まれている利用者公開鍵ＰＵによって暗号化し、その結果を、情報送受信手段４０２４により、ネットワーク４０４０を経由してＤＶＤ再生装置４０００に送信し、ステップ４４０８に進む。

【０２３３】次に、ステップ４４０８に示すように、ＤＶＤ再生装置４０００は情報送受信手段４００４により鍵管理サーバ４０２０からの暗号化されたデータを受信し、さらに、中央制御手段４００１の指示に従い、ＩＣカード駆動手段４０１０は、ＩＣカード４００９に格納されている利用者秘密鍵ＳＵを得て、この利用者秘密鍵ＳＵを用いて、データ暗号化鍵復号化手段４０１１により、データ暗号化鍵Ｄを得て、ステップ４４０９に進む。

【０２３４】次に、ステップ４４０９に示すように、ＤＶＤ内データ復号化手段４００８は既に得たデータ暗号化鍵Ｄを用いて、映画作品ＤＶＤ４００６上の暗号化されているデータを復号化し、情報表示手段４００３によって利用者に表示し、終了４４１２へ進む。

【０２３５】また、判断４４０３からステップ４４１０に進んだ場合には、鍵管理サーバ４０２０は、使用有効期限内ではないことを、情報送受信手段４０２４により、ネットワーク４０４０を経由して、ＤＶＤ再生装置４０００に送信し、ステップ４４１１に進む。

【０２３６】次に、ステップ４４１１に示すように、ＤＶＤ再生装置４０００の中央制御手段４００１は、使用有効期限内ではないことを、情報送受信手段４００４により受信し、情報表示手段４００３にこれを表示し、終了４４１２へ進む。

【０２３７】なお、本実施の形態においては可搬型メディアとしてＤＶＤ、メディア活用情報の記録領域としてＤＶＤ上のメディア活用情報記録領域を用いたが、可搬型メディアとしてフロッピーディスクやＰＤ、ＣＤ－ＲＯＭなどの他のメディアや、書換え可能型のＤＶＤを用い、メディア活用情報の記録領域については、メディア本体の記録領域を用いることも可能である。

【０２３８】このように、本実施の形態では、該可搬型メディアの使用有効期限を設定することが可能であるため、あらかじめ利用者から徴収した料金に見合う使用有

効期限を設定しておき、使用有効期限内である間は利用者の要求に応じてデータ暗号化鍵を渡して、可搬型メディアの使用の可否を制御することにより、可搬型メディアの無制限な利用を確実に防止でき、その実用的効果は大きい。

【０２３９】（実施の形態１１）次に、請求項２３に記載の発明に請求項２４に記載の発明の形態を結合させた第１１の実施の形態について説明する．図４５は、本実施の形態における、可搬型メディアとして暗号化された映画作品を記録した、視聴の都度、鍵管理サーバに有効期限の確認を行ない、使用有効期限内である場合にのみ、鍵管理サーバから、復号用のデータ暗号化鍵を得ることが可能であるような、映画作品再生システムの構成を示す図である。

【０２４０】図４５において、４５００はＤＶＤ再生装置である。４５０１は前記ＤＶＤ再生装置４５００の動作全体を制御する中央制御手段、４５０２は前記ＤＶＤ再生装置４５００に対して利用者が入力を行なうキーボードやマウス、音声認識装置、タブレット、ペン、ボタン、リモートコントロールボタンなどの入力手段、４５０３は利用者に対して前記ＤＶＤ再生装置４５００が表示を行なうためのディスプレイ、スピーカなどの情報表示手段、４５０４は前記ＤＶＤ再生装置４５００のネットワークに対する情報の送受信を行なう情報送受信手段、４５０５は前記情報送受信手段４５０４などから得られる情報を一時的に記憶しておく情報記憶手段である。４５０６は映画作品をデータ暗号化鍵Ｄで暗号化して記録した映画作品ＤＶＤであって、そのメディア活用情報記録領域には、映画作品ＤＶＤの種類を特定可能なタイトル情報と、タイトル情報ごとの発行番号情報が記録されている。４５０７は前記映画作品ＤＶＤ４５０６を駆動するＤＶＤ駆動手段である。４５０８は前記データ暗号化鍵Ｄを用いて前記映画作品ＤＶＤ４５０６内の暗号化された映画作品を復号化するＤＶＤ内データ復号化手段である。４５０９は公開鍵暗号方式における、前記利用者の公開鍵に対応する利用者の秘密鍵が記録されているＩＣカード、４５１０は前記ＩＣカード４５０９を駆動するＩＣカード駆動手段である。４５１１は前記利用者の秘密鍵を用いて、前記暗号化データ暗号化鍵を復号化してデータ暗号化鍵Ｄを生成するデータ暗号化鍵復号化手段、４５１２は鍵管理サーバにデータを送信する際に、鍵管理サーバの公開鍵を用いてデータを暗号化し、暗号化データとする、送信データ暗号化手段である。

【０２４１】４５２０は映画作品ＤＶＤ４５０６に記録されている映画作品の鍵管理サーバである。４５２１は前記鍵管理サーバ４５２０の動作全体を制御する中央制御手段、４５２４は前記鍵管理サーバ４５２０のネットワークに対する情報の送受信を行なう情報送受信手段、４５２５は前記情報送受信手段４５２４などから得られる情報や、鍵管理サーバ４５２０自身で生成した情報を一時的に記憶しておく情報記憶手段である。４５２９は公開鍵暗号方式における、前記鍵管理サーバの公開鍵に対応する鍵管理サーバの秘密鍵が記録されているＩＣカード、４５３０は前記ＩＣカード４５２９を駆動するＩＣカード駆動手段である。４５３１は前記鍵管理サーバの秘密鍵を用いて、前記ＤＶＤ再生装置４５００から送信されてきた暗号化データを復号化する受信データ復号化手段である。４５３２は利用者に対して送信するデータ暗号化鍵を公開鍵暗号方式における利用者の公開鍵で暗号化する送信データ暗号化手段、４５３３は前記送信データ暗号化手段４５１２と、前記送信データ暗号化手段４５３２とにおいて利用する乱数を発生させる乱数発生手段、４５３４は映画作品ＤＶＤの使用有効期限情報と利用者の公開鍵とを前記タイトル情報と前記発行番号情報とによって管理する利用者情報管理手段、４５３５は前記データ暗号化鍵を前記タイトル情報によって管理するＤＶＤ情報管理手段、４５３６は現在時刻を発生させる現在時刻発生手段、４５３７は現在時刻発生手段４５３６によって得られた現在時刻と使用有効期限とを比較し、映画作品ＤＶＤが使用有効期限内であるかどうかを判断する使用有効期限判断手段である。４５４０は前記ＤＶＤ再生装置４５００と前記鍵管理サーバ４５２０との間を繋ぐネットワークである。

【０２４２】図４６は、本実施の形態にかかわるメディア活用情報の構成例である。図４６において、４６００はメディア活用情報、メディア活用情報４６００のうち、４６０１は映画作品ＤＶＤの種類を特定可能なタイトル情報、４６０２は該映画作品ＤＶＤを他のものと識別可能な、前記タイトル情報ごとの発行番号情報、４６０４は鍵管理サーバの、公開鍵暗号方式における公開鍵を含む、鍵管理サーバ公開鍵情報であり、映画作品ＤＶＤ配布時には既に前記メディア活用情報記録領域に記録済みである。

【０２４３】図４７は、本実施の形態にかかわる利用者情報の構成例である。図４７において、４７００は利用者情報、４７０１は前記メディア活用情報４６００内に含まれるタイトル情報、４７０２は前記メディア活用情報４６００内に含まれる発行番号情報、４７０３は前記タイトル情報４７０１と前記発行番号情報４７０２とで特定可能な映画作品ＤＶＤを保有している利用者の、公開鍵暗号方式における公開鍵を含む利用者公開鍵情報、４７０６は前記タイトル情報４７０１と前記発行番号情報４７０２によって特定可能な可搬型メディアの使用有効期限を示す、使用有効期限情報であって、可搬型メディアごとに異なっていてもよいものである。ここで、図４７においては、一つのエントリのみ示したが、実際には、このような形式で複数のエントリが存在する。これらは前記利用者情報管理手段４５３４によって管理されている。

【０２４４】図４８は、本実施の形態にかかわるＤＶＤ情報の構成例である。図４８において、４８００はＤＶＤ情報、４８０１は前記メディア活用情報４６００内に含まれるタイトル情報、４８０２はこのタイトル情報４８０１によって特定可能な種類の映画作品ＤＶＤ内に記録されている映画作品を暗号化するのに用いたデータ暗号化鍵Ｄを含むデータ暗号化鍵情報である。ここで、図４８においては、一つのエントリのみ示したが、実際には、このような形式で複数のエントリが存在する。これらは前記ＤＶＤ情報管理手段４５３５によって管理されている。

【０２４５】図４９は、本実施の形態の処理の流れを示すフローチャートである。以下、図４５から図４９を用いて本実施の形態の動作を説明する。

【０２４６】利用者は書店や通信販売で購入、あるいは会員制のサービスによって配布してもらうことにより映画作品ＤＶＤ４５０６を入手する。

【０２４７】以降、利用者が映画作品ＤＶＤを再生する場合の、使用有効期限の管理と、使用有効期限を超えない場合のデータ暗号化鍵の取得と取得の依頼とを安全に行なう方法について、図４９のフローチャートに沿って説明する。なお、図４９においては角の丸い長方形で囲われた部分は、フローチャートの開始・終了を示し、長方形で囲われた部分は処理を示し、菱形で囲われた部分は判断を示し、矢印は処理の流れを示している。

【０２４８】まず、利用者は、映画作品ＤＶＤ４５０６をＤＶＤ再生装置４５００のＤＶＤ駆動手段４５０７にセットし、入力手段４５０２を用いて、再生開始をＤＶＤ再生装置４５００の中央制御手段４５０１に指示する。これにより、開始４９００に示すように、映画作品ＤＶＤの再生処理が開始される。

【０２４９】まず、ステップ４９０１に示すように、ＤＶＤ再生装置４５００の中央制御手段４５０１は、情報送受信手段４５０４により、ネットワーク４５４０を経由して、鍵管理サーバ４５２０に対して、乱数の取得を依頼し、ステップ４９０２に進む。

【０２５０】次に、ステップ４９０２に示すように、鍵管理サーバ４５２０の中央制御手段４５２１は、乱数取得依頼の指示を、情報送受信手段４５２４により受信し、乱数発生手段４５３３により乱数Ｒを発生させ、情報記憶手段４５２５に乱数Ｒを記憶させ、乱数Ｒを、情報送受信手段４５２４により、ネットワーク４５４０を経由して、ＤＶＤ再生装置４５００に送信し、ステップ４９０３に進む。

【０２５１】次に、ステップ４９０３に示すように、ＤＶＤ再生装置４５００の中央制御手段４５０１は、乱数Ｒを情報送受信手段４５０４により受信し、乱数Ｒは情報記憶手段４５０５に記憶させ、送信データ暗号化手段４５１２は、乱数Ｒと、ＤＶＤ駆動手段４５０７によって映画作品ＤＶＤ４５０６のメディア活用情報４６００から得られる鍵管理サーバ公開鍵情報４６０４に含まれている鍵管理サーバ公開鍵ＰＳとを用いて、同じく映画作品ＤＶＤ４５０６のメディア活用情報４６００から得られるタイトル情報４６０１と発行番号情報４６０２とを暗号化し、ステップ４９０４に進む。

【０２５２】次に、ステップ４９０４に示すように、ＤＶＤ再生装置４５００の中央制御手段４５０１の指示により、情報送受信手段４５０４により、ネットワーク４５４０を経由して、鍵管理サーバ４５２０に対して、暗号化されたタイトル情報４６０１と発行番号情報４６０２とを送信し、データ暗号化鍵の取得を鍵管理サーバ４５２０に依頼し、ステップ４９０５に進む。

【０２５３】次に、ステップ４９０５に示すように、鍵管理サーバ４５２０は情報送受信手段４５２４によりＤＶＤ再生装置４５００からの暗号化されたデータを受信し、さらに、中央制御手段４５２１の指示に従い、ＩＣカード駆動手段４５３０は、ＩＣカード４５２９に格納されている鍵管理サーバ秘密鍵ＳＳを得て、受信データ復号化手段４５３１により、タイトル情報４６０１と発行番号情報４６０２とを復号化し、判断４９０６に進む。

【０２５４】次に、判断４９０６に示すように、ステップ４９０５において、送信されたデータから得られた乱数Ｒが情報記憶手段４５２５に記憶してある乱数と等しいかどうかを判断し、等しい場合には、Ｒを用いて正しく復号化できたものとしてステップ４９０７に進み、等しくない場合には正しく復号化できなかったものとしてステップ４９１２に進む。

【０２５５】ステップ４９０７に進んだ場合には、鍵管理サーバ４５２０の中央制御手段４５２１は、ステップ４９０５で得たタイトル情報４６０１と発行番号情報４６０２とを用いて、利用者情報管理手段４５３４に対して、タイトル情報４６０１と発行番号情報４６０２とで管理されている利用者情報のエントリ４７００を得て、その使用有効期限情報４７０６を得、また、現在時刻発生手段４５３６により、現在時刻Ｃを得て、判断４９０８に進む。ここで、利用者情報４７００のうちのタイトル情報４７０１と発行番号情報４７０２とは、それぞれ前記タイトル情報４６０１と前記発行番号情報４６０２とに等しい。

【０２５６】次に、判断４９０８に示すように、使用有効期限判断手段４５３７において、現在時刻Ｃが、前記得られた使用有効期限情報４７０６に含まれている有効期限内であるかどうかを判断し、有効期限内である場合には、ステップ４９０９に進み、有効期限外である場合には、ステップ４９１３に進む。

【０２５７】ステップ４９０９に進んだ場合には、ＤＶＤ情報管理手段４５３５は、タイトル情報４６０１を元に、ＤＶＤ情報４８００からデータ暗号化鍵情報４８０２を得、利用者情報管理手段４５３４は、タイトル情報

４６０１と発行番号情報４６０２とを元に、利用者公開鍵情報４７０３を得て、ステップ４９１０に進む。ここで、ＤＶＤ情報４８００のうちのタイトル情報４８０１は、前記タイトル情報４６０１と等しい。

【０２５８】次に、ステップ４９１０に示すように、送信データ暗号化手段４５３２において、情報記憶手段４５２５に記憶してある乱数Ｒを用いて、前記データ暗号化鍵情報４８０２に含まれているデータ暗号化鍵Ｄを暗号化し、さらに、Ｒと前記暗号化されたＤとを組合せたデータを、ステップ４９０９で得られた利用者公開鍵情報４７０３に含まれている利用者公開鍵ＰＵによって暗号化し、その結果を、情報送受信手段４５２４により、ネットワーク４５４０を経由してＤＶＤ再生装置４５００に送信し、ステップ４９１１に進む。

【０２５９】次に、ステップ４９１１に示すように、ＤＶＤ再生装置４５００は情報送受信手段４５０４により鍵管理サーバ４５２０からの暗号化されたデータを受信し、さらに、中央制御手段４５０１の指示に従い、ＩＣカード駆動手段４５１０は、ＩＣカード４５０９に格納されている利用者秘密鍵ＳＵを得て、この利用者秘密鍵ＳＵを用いて、データ暗号化鍵復号化手段４５１１により、データ暗号化鍵Ｄを得て、ＤＶＤ内データ復号化手段４５０８において、データ暗号化鍵Ｄを用いて、映画作品ＤＶＤ４５０６上の暗号化されているデータを復号化し、情報表示手段４５０３によって利用者に表示し、終了４９１５へ進む。

【０２６０】また、判断４９０６からステップ４９１２に進んだ場合には、ネットワークの障害によってＲの値が正しく送信されなかったか、あるいは不正な利用者が介在したために、Ｒの値が正しく送信されなかったかのどちらかであるとし、処理を中断する。

【０２６１】また、判断４９０８からステップ４９１３に進んだ場合には、鍵管理サーバ４５２０は、使用有効期限内ではないことを、情報送受信手段４５２４により、ネットワーク４５４０を経由して、ＤＶＤ再生装置４５００に送信し、ステップ４９１４に進む。

【０２６２】次に、ステップ４９１４に示すように、ＤＶＤ再生装置４５００の中央制御手段４５０１は、使用有効期限内ではないことを、情報送受信手段４５０４により受信し、情報表示手段４５０３にこれを表示し、終了４９１５へ進む。

【０２６３】なお、本実施の形態においては可搬型メディアとしてＤＶＤ、メディア活用情報の記録領域としてＤＶＤ上のメディア活用情報記録領域を用いたが、可搬型メディアとしてフロッピーディスクやＰＤ、ＣＤ－ＲＯＭなどの他のメディアや、書換え可能型のＤＶＤを用い、メディア活用情報の記録領域については、メディア本体の記録領域を用いることも可能である。

【０２６４】このように、本実施の形態では、該可搬型メディアの使用有効期限を設定することが可能であるため、あらかじめ利用者から徴収した料金に見合う使用有効期限を設定しておき、使用有効期限内である間は利用者の要求に応じてデータ暗号化鍵を渡して、可搬型メディアの使用の可否を制御することにより、可搬型メディアの無制限な利用を確実に防止するという効果を奏するもので、かつ、利用者の要求を鍵管理サーバに送信する場合には、タイトル情報や発行番号情報などの機密の情報が第三者に漏洩することのないように、暗号化して送信することで、安全なデータ転送をも可能にし、その実用的効果は大きい。

【０２６５】

【発明の効果】以上のように本発明によれば、第１に、大容量のデータの記録が可能な可搬型メディア内の暗号化データを復号化するのに必要なデータ暗号化鍵を利用者ごとの秘密情報で解読可能な形式で暗号化して、暗号化データ暗号化鍵とし、この暗号化データ暗号化鍵を、該可搬型メディアそれぞれに固有なメディア活用情報として記録しておき、利用者ごとの秘密情報は別途格納しておくことを特徴とする可搬型メディアの駆動装置であり、可搬型メディア内の暗号化データを復号化する際には、まず利用者ごとの秘密情報を得て、これによって可搬型メディアのメディア活用情報内の暗号化データ暗号化鍵を復号化してデータ暗号化鍵とし、さらにこのデータ暗号化鍵によって可搬型メディア内の暗号化データを復号化する構成としたことにより、可搬型メディアを利用できるのは、あらかじめ特定された利用者であって、かつ、利用の際には利用者ごとの秘密情報を必要とするため、可搬型メディアを単独では利用することができず、結果として不正な利用を防止し、さらに、メディア活用情報まで含めて不正に複製しても特定された利用者の秘密情報がなければ利用できないため、結果として不正な複製を防止できるという効果を奏する。

【０２６６】第２に、大容量のデータの記録が可能な可搬型メディア内の暗号化データを復号化するのに必要なデータ暗号化鍵を、可搬型メディアのメディア活用情報に記録されているタイトル情報ごとにサーバ側で管理しておき、また、利用者の秘密情報と一対の公開の情報を前記タイトル情報とタイトル情報ごとの発行番号情報ごとにサーバ側で管理しておき、利用者の秘密情報は別途格納しておいてクライアント側で利用することを特徴とする可搬型メディアとネットワークの連携装置であり、利用者はメディア活用情報に記録されているタイトル情報と発行番号情報をサーバ側に通知してデータ暗号化鍵の取得を依頼し、サーバ側は得られたタイトル情報に対応するデータ暗号化鍵を、得られたタイトル情報と発行番号情報に対応する公開の情報と、別途発生させる乱数を用いて暗号化して送り返し、利用者側では利用者ごとの秘密情報を用いて、得られたデータから乱数を分離し、さらにデータ暗号化鍵を得て、暗号化データを復号化して利用する構成としたことにより、可搬型メディア

を利用できるのは、タイトル情報・発行番号情報と、利用者の保持する秘密情報と一対の公開の情報を登録済みの特定された利用者であって、かつ、利用の際には利用者ごとの秘密情報を必要とするため、可搬型メディアを単独では利用することができず、結果として不正な利用を防止し、さらに、メディア活用情報まで含めて不正に複製しても特定された利用者の秘密情報がなければ利用できないため、結果として不正な複製を防止するとともに悪意の利用者のなりすましを防止できるという効果を奏する。

【０２６７】第３に、可搬型メディアのメディア活用情報にサーバの秘密情報と一対の公開情報を記録しておき、サーバの秘密情報は別途格納しておいてサーバ側で利用することを特徴とする可搬型メディアとネットワークの連携装置であり、利用者からサーバにデータを送信する際には、サーバで別途発生させる乱数と、メディア活用情報内の公開情報を用いて暗号化して送信し、サーバ側では、サーバの秘密情報と前記乱数を用いて得られたデータの正当性を確認したのち、乱数を分離して、利用者からデータを得る構成としたことにより、利用者からサーバに安全にデータを送信する際に必要とする、サーバの公開鍵の取得が容易であるという効果に加え、サーバの公開鍵が可搬型メディアごとに異なるものであっても良いという効果を奏する。

【０２６８】第４に、可搬型メディアそれぞれに固有のメディア活用情報としてタイトル情報とタイトル情報ごとの発行番号情報を設け、このタイトル情報と発行番号情報とを用いてサーバ側で可搬型メディアの使用量を管理することを特徴とする可搬型メディアとネットワークの連携装置であり、可搬型メディアを利用する際には、メディア活用情報内のタイトル情報と発行番号情報とをサーバに送信し、サーバ側では該可搬型メディアの使用量を加算したり、また、最大使用量が設定されている場合には、それを超えるかどうかの判断を行なう構成としたことにより、該可搬型メディアの使用量をもとに利用料金を利用者に対して請求したり、また、あらかじめ利用料金を払い込んである場合に、それに応じた最大使用量を超える場合にはその旨通知したりといったことが可能であって、可搬型メディアの無制限な利用を防止するという効果を奏する。

【０２６９】第５に、前記第２の構成と前記第４の構成とを組合せた可搬型メディアとネットワークの連携装置であり、常にデータ暗号化鍵をサーバから取得するようにし、最大使用量を超える場合にはデータ暗号化鍵を渡さないようにする構成としたことにより、最大使用量を超えての可搬型メディアの無制限な利用を確実に防止するという効果を奏する。

【０２７０】第６に、前記第３の構成と前記第５の構成とを組合せた可搬型メディアとネットワークの連携装置であり、データ暗号化鍵取得のためのメディア活用情報を暗号化して送信する構成としたことにより、メディア活用情報に記述されている情報を安全にサーバに送信することが可能であるという効果を奏する。

【０２７１】第７に、可搬型メディアそれぞれに固有のメディア活用情報として使用有効期限情報を設け、サーバ側には、使用有効期限を判断する手段を設けたことを特徴とする可搬型メディアとネットワークの連携装置、あるいは、可搬型メディアそれぞれに固有のメディア活用情報としてタイトル情報、あるいはタイトル情報とタイトル情報ごとの発行番号情報とを設け、サーバ側には、タイトル情報、あるいはタイトル情報とタイトル情報ごとの発行番号情報とによって該可搬型メディアの使用有効期限を管理する手段と、使用有効期限を判断する手段を設けたことを特徴とする可搬型メディアとネットワークの連携装置であって、可搬型メディアを利用する際には、メディア活用情報内の使用有効期限情報、あるいはタイトル情報、あるいはタイトル情報と発行番号情報とをサーバに送信し、サーバ側で該可搬型メディアが使用可能かどうかを判断することを特徴としたことにより、可搬型メディアに対してあらかじめ使用有効期限を設定した場合に、それを超えて該可搬型を利用しようとする場合にその旨通知したり、また、あらかじめ利用料金を払い込んである場合に、それに応じた利用期間を超える場合にはその旨通知したりといったことが可能であって、可搬型メディアの無制限な利用を防止するという効果が得られる。

【０２７２】第８に、前記第２の構成と前記第７の構成とを組合せた可搬型メディアとネットワークの連携装置であり、常にデータ暗号化鍵をサーバから取得するようにし、使用有効期限を超える場合にはデータ暗号化鍵を渡さないようにする構成としたことにより、使用有効期限を超えての可搬型メディアの無制限な利用を確実に防止するという効果を奏する。

【０２７３】第９に、前記第３の構成と前記第８の構成とを組合せた可搬型メディアとネットワークの連携装置であり、データ暗号化鍵取得のためのメディア活用情報を暗号化して送信する構成としたことにより、メディア活用情報に記述されている情報を安全にサーバに送信できるという効果を奏する。

【図面の簡単な説明】

【図１】本発明の第１の実施の形態における構成例を示す図

【図２】本発明の第１の実施の形態におけるメディア活用情報の構成例を示す図

【図３】本発明の第１の実施の形態における動作のフローチャートを示す図

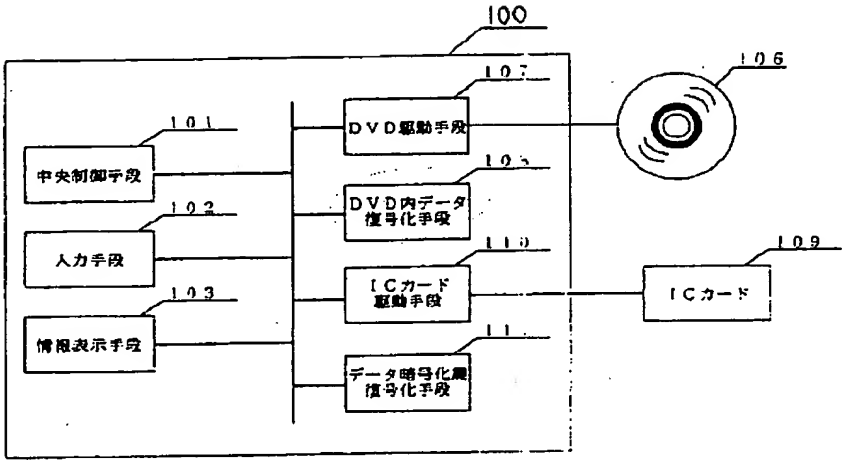
【図４】本発明の第２の実施の形態における構成例を示す図

【図５】本発明の第２の実施の形態におけるメディア活用情報の構成例を示す図

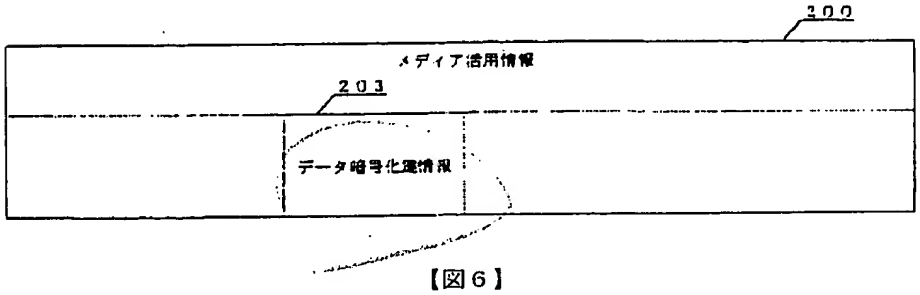
【図６】本発明の第２の実施の形態における利用者情報の構成例を示す図
【図７】本発明の第２の実施の形態におけるＤＶＤ情報の構成例を示す図
【図８】本発明の第２の実施の形態における動作のフローチャートを示す図
【図９】本発明の第３の実施の形態における構成例を示す図
【図１０】本発明の第３の実施の形態におけるメディア活用情報の構成例を示す図
【図１１】本発明の第３の実施の形態におけるＤＶＤ情報の構成例を示す図
【図１２】本発明の第３の実施の形態における動作のフローチャートを示す図
【図１３】本発明の第４の実施の形態における構成例を示す図
【図１４】本発明の第４の実施の形態におけるメディア活用情報の構成例を示す図
【図１５】本発明の第４の実施の形態における利用者情報の構成例を示す図
【図１６】本発明の第４の実施の形態における動作のフローチャートを示す図
【図１７】本発明の第４の実施の形態における利用者情報の構成の他の例を示す図
【図１８】本発明の第５の実施の形態における利用者情報の構成の例を示す図
【図１９】本発明の第５の実施の形態における動作のフローチャートを示す図
【図２０】本発明の第５の実施の形態におけるメディア活用情報の構成の他の例を示す図
【図２１】本発明の第５の実施の形態における他の動作のフローチャートを示す図
【図２２】本発明の第６の実施の形態における構成例を示す図
【図２３】本発明の第６の実施の形態におけるメディア活用情報の構成例を示す図
【図２４】本発明の第６の実施の形態における利用者情報の構成例を示す図
【図２５】本発明の第６の実施の形態におけるＤＶＤ情報の構成例を示す図
【図２６】本発明の第６の実施の形態における動作のフローチャートを示す図
【図２７】本発明の第７の実施の形態における構成例を示す図
【図２８】本発明の第７の実施の形態におけるメディア活用情報の構成例を示す図
【図２９】本発明の第７の実施の形態における利用者情報の構成例を示す図
【図３０】本発明の第７の実施の形態におけるＤＶＤ情報の構成例を示す図
【図３１】本発明の第７の実施の形態における動作のフローチャートを示す図
【図３２】本発明の第８の実施の形態における構成例を示す図
【図３３】本発明の第８の実施の形態におけるメディア活用情報の構成例を示す図
【図３４】本発明の第８の実施の形態における利用者情報の構成例を示す図
【図３５】本発明の第８の実施の形態における動作のフローチャートを示す図
【図３６】本発明の第９の実施の形態における構成の例を示す図
【図３７】本発明の第９の実施の形態におけるメディア活用情報の構成の例を示す図
【図３８】本発明の第９の実施の形態における動作のフローチャートを示す図
【図３９】本発明の第８の実施の形態における利用者情報の構成の他の例を示す図
【図４０】本発明の第１０の実施の形態における構成例を示す図
【図４１】本発明の第１０の実施の形態におけるメディア活用情報の構成例を示す図
【図４２】本発明の第１０の実施の形態における利用者情報の構成例を示す図
【図４３】本発明の第１０の実施の形態におけるＤＶＤ情報の構成例を示す図
【図４４】本発明の第１０の実施の形態における動作のフローチャートを示す図
【図４５】本発明の第１１の実施の形態における構成例を示す図
【図４６】本発明の第１１の実施の形態におけるメディア活用情報の構成例を示す図
【図４７】本発明の第１１の実施の形態における利用者情報の構成例を示す図
【図４８】本発明の第１１の実施の形態におけるＤＶＤ情報の構成例を示す図
【図４９】本発明の第１１の実施の形態における動作のフローチャートを示す図
【符号の説明】
２００　メディア活用情報
２０３　データ暗号化鍵情報
５０１　タイトル情報
５０２　発行番号情報
６００　利用者情報
６０３　利用者公開鍵情報
７００　ＤＶＤ情報
１０００　料金サーバ公開情報
１１０３　料金情報
１５０４　使用量累計
１７０７　映画作品名

１８０４　使用量累計
１８０５　最大使用量
３４０６　使用有効期限情報
４５００　ＤＶＤ再生装置
４５０１　中央制御手段
４５０２　入力手段
４５０３　情報表示手段
４５０４　情報送受信手段
４５０５　情報記憶手段
４５０６　映画作品ＤＶＤ
４５０７　ＤＶＤ駆動手段
４５０８　ＤＶＤ内データ復号化手段
４５０９　ＩＣカード
４５１０　ＩＣカード駆動手段
４５１１　データ暗号化鍵復号化手段
４５１２　送信データ暗号化手段
４５２０　鍵管理サーバ
４５２１　中央制御手段
４５２４　情報送受信手段
４５２５　情報記憶手段
４５２９　ＩＣカード
４５３０　ＩＣカード駆動手段
４５３１　受信データ復号化手段
４５３２　送信データ暗号化手段
４５３３　乱数発生手段
４５３４　利用者情報管理手段
４５３５　ＤＶＤ情報管理手段
４５３６　現在時刻発生手段
４５３７　使用有効期限判断手段
４５４０　ネットワーク

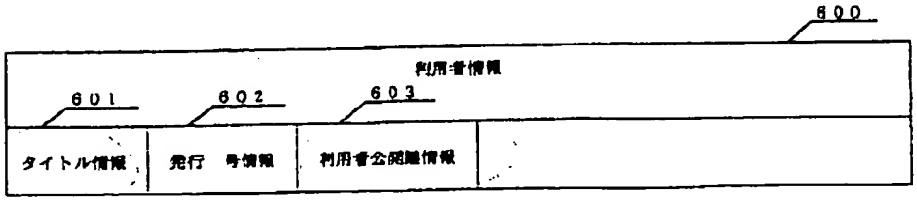
【図１】



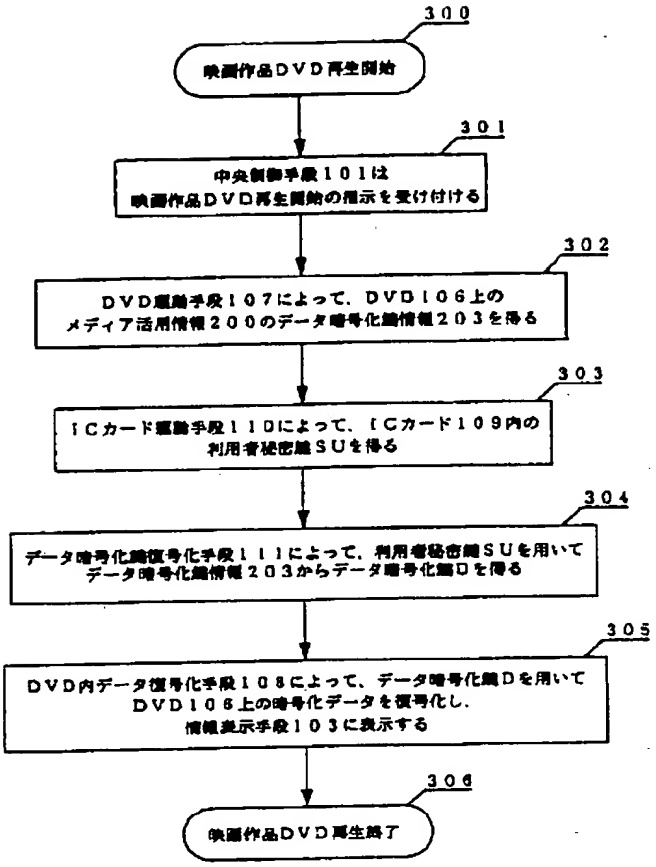
【図２】



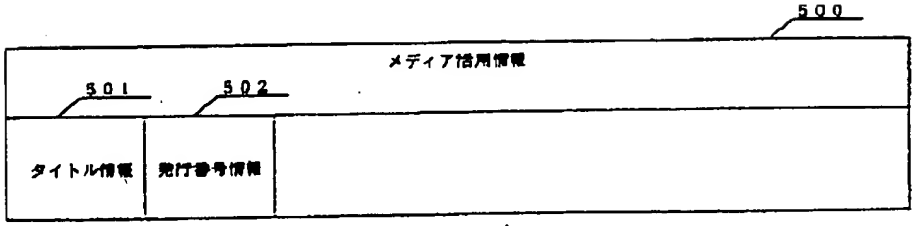
【図６】



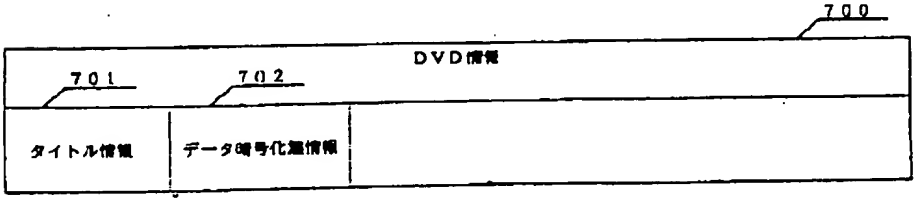
【図３】


300
映画作品ＤＶＤ再生開始
301
中央制御手段１０１は
映画作品ＤＶＤ再生開始の指示を受け付ける
302
ＤＶＤ読取手段１０７によって、ＤＶＤ１０６上の
メディア活用情報２００のデータ暗号化鍵情報２０３を得る
303
ＩＣカード読取手段１１０によって、ＩＣカード１０９内の
利用者秘密鍵ＳＵを得る
304
データ暗号化鍵復号化手段１１１によって、利用者秘密鍵ＳＵを用いて
データ暗号化鍵情報２０３からデータ暗号化鍵Ｄを得る
305
ＤＶＤ内データ復号化手段１０８によって、データ暗号化鍵Ｄを用いて
ＤＶＤ１０６上の暗号化データを復号化し、
情報表示手段１０３に表示する
306
映画作品ＤＶＤ再生終了

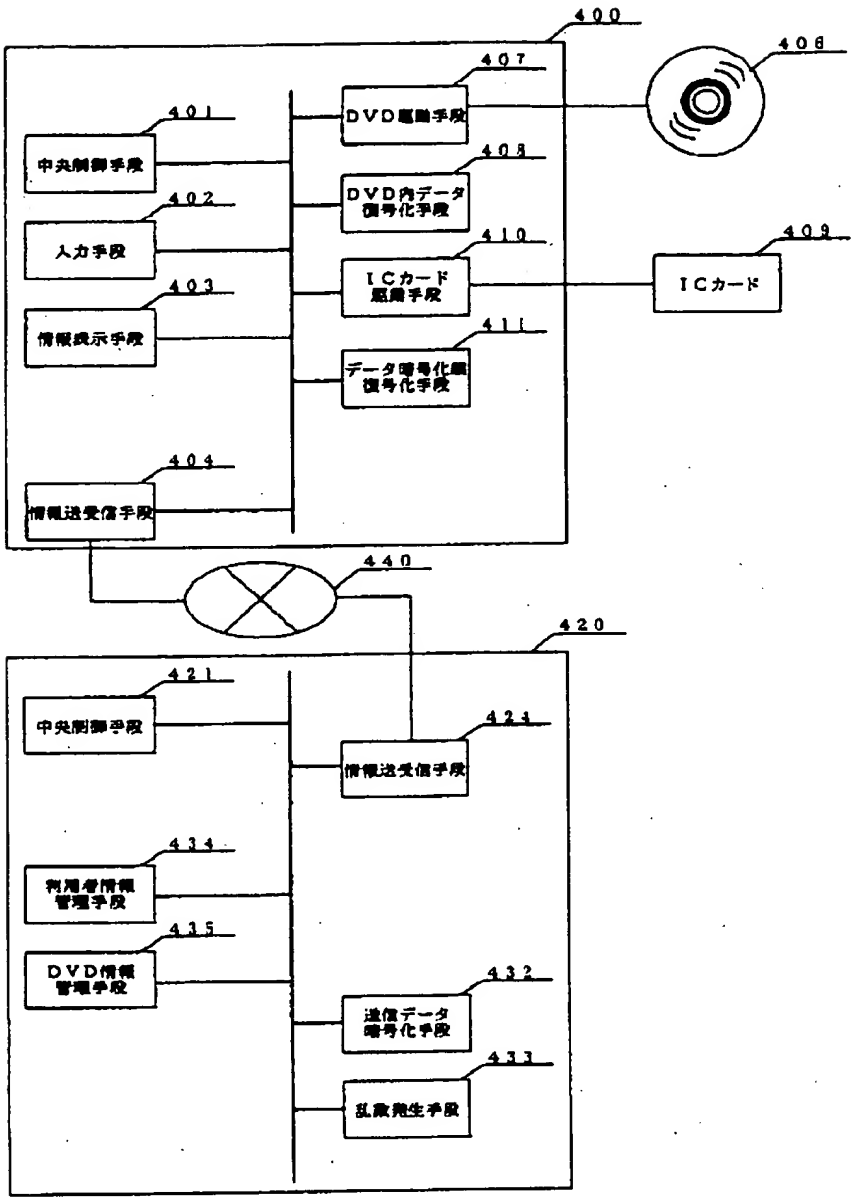
【図５】


500
メディア活用情報
501
502
タイトル情報
発行番号情報

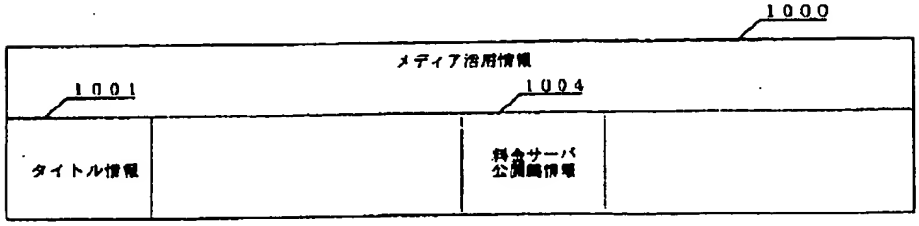
【図７】


700
ＤＶＤ情報
701
702
タイトル情報
データ暗号化鍵情報

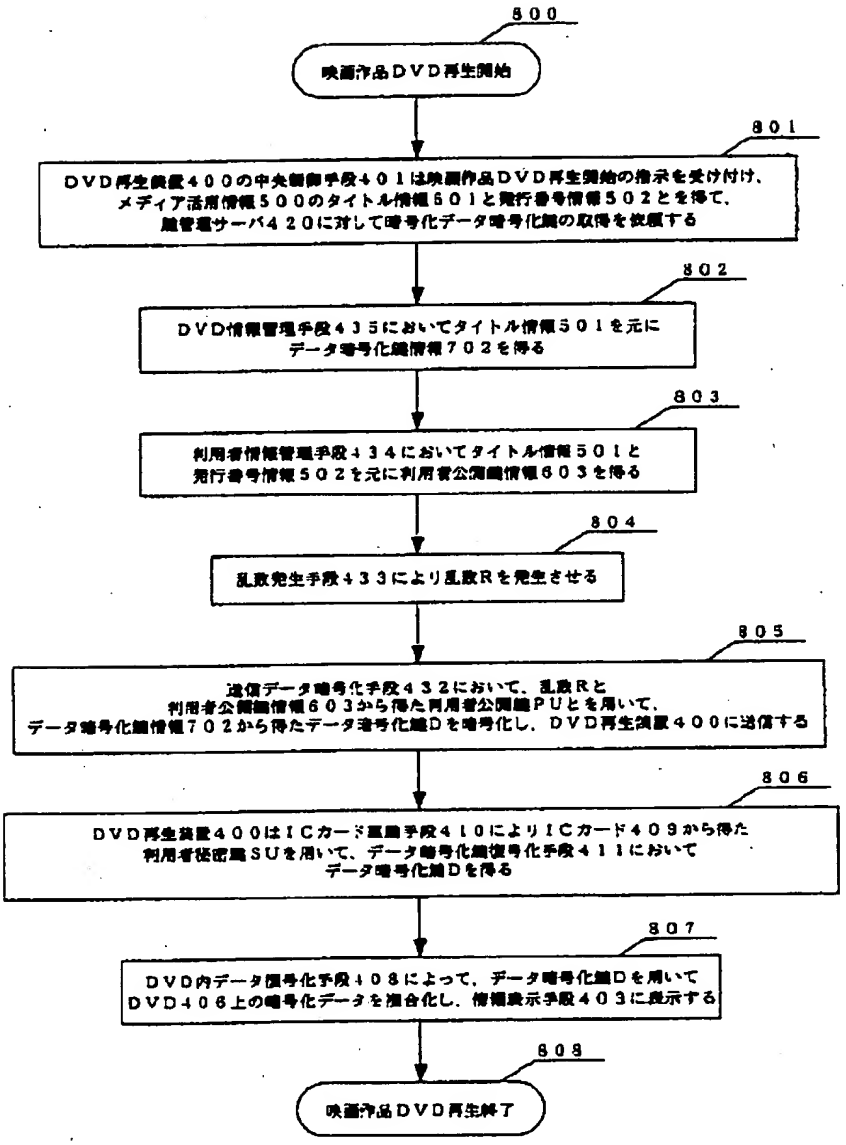
【図４】


400
406
407
DVD駆動手段
401
中央制御手段
408
DVD内データ復号化手段
402
入力手段
410
409
ICカード駆動手段
ICカード
403
情報提示手段
411
データ暗号化鍵復号化手段
404
情報送受信手段
440
420
421
中央制御手段
424
情報送受信手段
434
利用者情報管理手段
435
DVD情報管理手段
432
送信データ暗号化手段
433
乱数発生手段

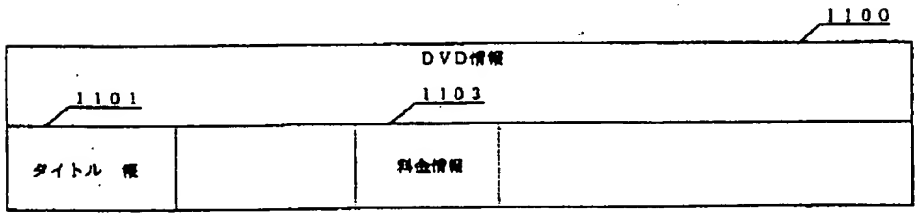
【図１０】


1000
メディア活用情報
1001
1004
タイトル情報
料金サーバ公開鍵情報

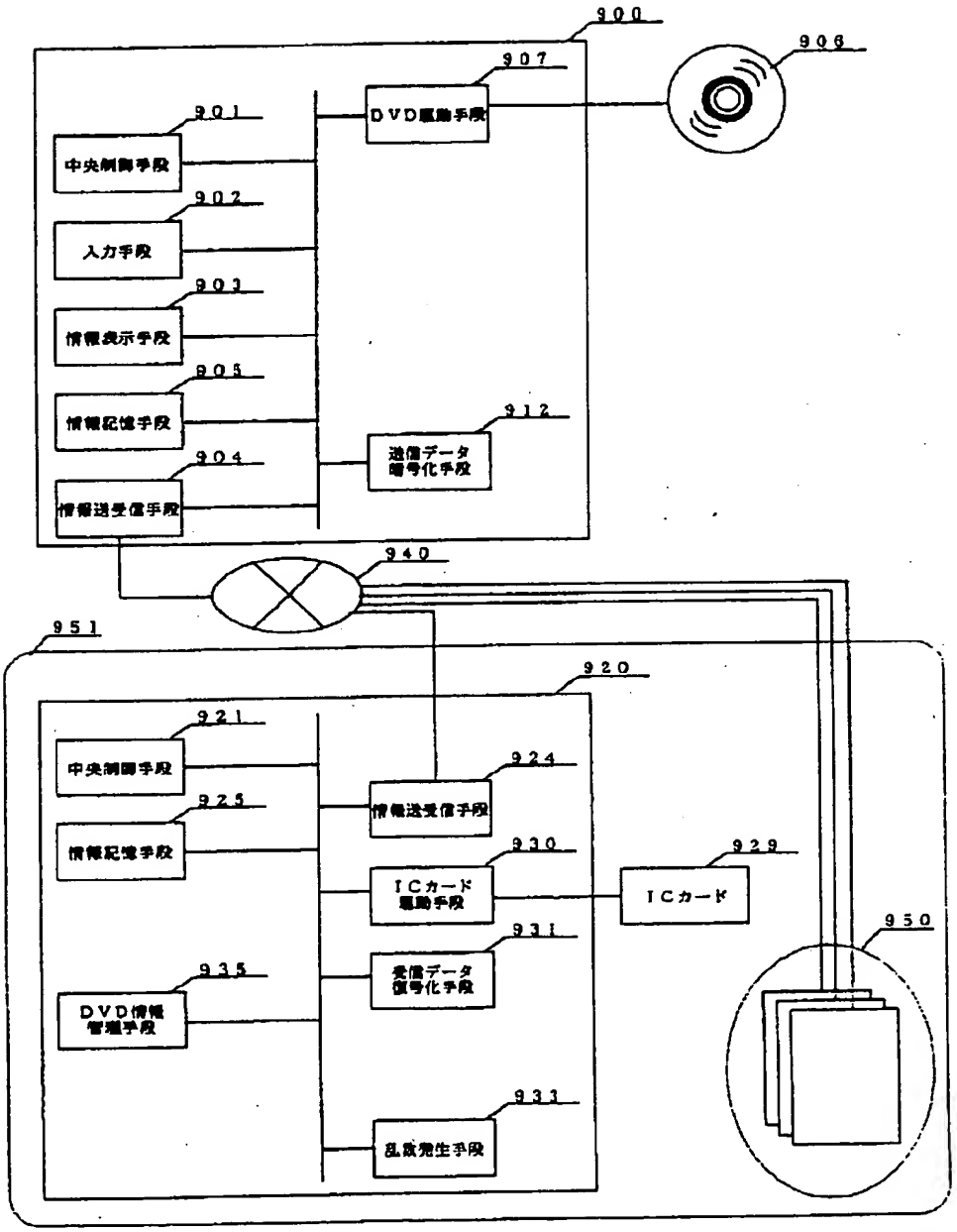
【図８】


８００
映画作品ＤＶＤ再生開始
８０１
ＤＶＤ再生装置４００の中央制御手段４０１は映画作品ＤＶＤ再生開始の指示を受け付け、
メディア活用情報５００のタイトル情報５０１と発行番号情報５０２とを得て、
鍵管理サーバ４２０に対して暗号化データ暗号化鍵の取得を依頼する
８０２
ＤＶＤ情報管理手段４３５においてタイトル情報５０１を元に
データ暗号化鍵情報７０２を得る
８０３
利用者情報管理手段４３４においてタイトル情報５０１と
発行番号情報５０２を元に利用者公開鍵情報６０３を得る
８０４
乱数発生手段４３３により乱数Ｒを発生させる
８０５
送信データ暗号化手段４３２において、乱数Ｒと
利用者公開鍵情報６０３から得た利用者公開鍵ＰＵとを用いて、
データ暗号化鍵情報７０２から得たデータ暗号化鍵Ｄを暗号化し、ＤＶＤ再生装置４００に送信する
８０６
ＤＶＤ再生装置４００はＩＣカード処理手段４１０によりＩＣカード４０９から得た
利用者秘密鍵ＳＵを用いて、データ暗号化鍵復号化手段４１１において
データ暗号化鍵Ｄを得る
８０７
ＤＶＤ内データ復号化手段４０８によって、データ暗号化鍵Ｄを用いて
ＤＶＤ４０６上の暗号化データを復合化し、情報表示手段４０３に表示する
８０８
映画作品ＤＶＤ再生終了

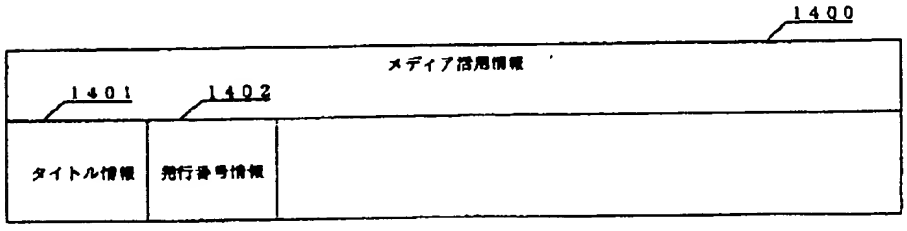
【図１１】


１１００
ＤＶＤ情報
１１０１
１１０３
タイトル　情報
料金情報

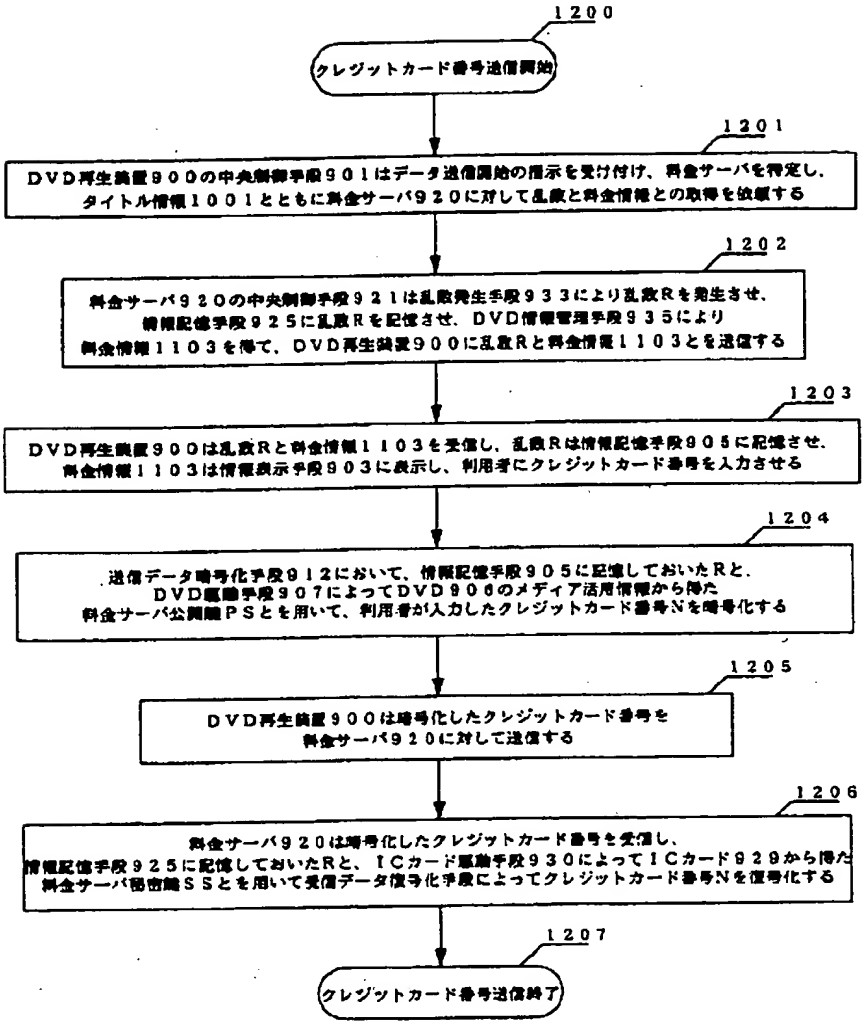
【図９】


900
906
907
DVD駆動手段
901
中央制御手段
902
入力手段
903
情報表示手段
905
情報記憶手段
912
送信データ暗号化手段
904
情報送受信手段
940
951
920
921
中央制御手段
924
情報送受信手段
925
情報記憶手段
930
ICカード駆動手段
929
ICカード
931
受信データ復号化手段
950
935
DVD情報管理手段
933
乱数発生手段

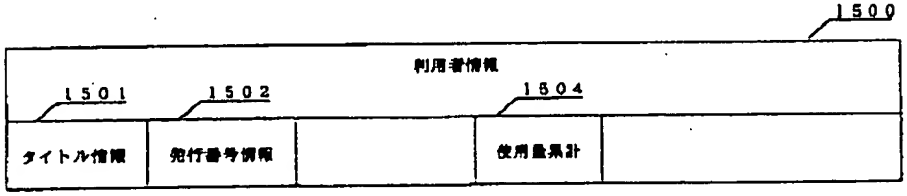
【図１４】


1400
メディア活用情報
1401
1402
タイトル情報
発行番号情報

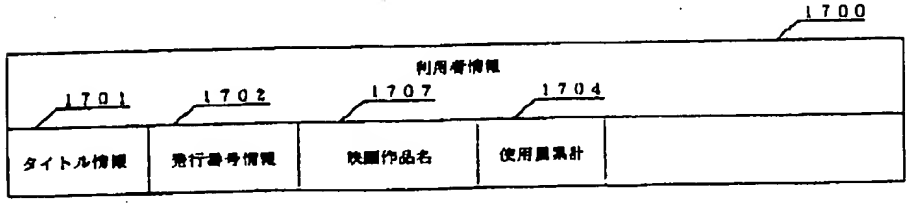
【図１２】


1200
クレジットカード番号送信開始
1201
DVD再生装置９００の中央制御手段９０１はデータ送信開始の指示を受け付け、料金サーバを特定し、
タイトル情報１００１とともに料金サーバ９２０に対して乱数と料金情報との取得を依頼する
1202
料金サーバ９２０の中央制御手段９２１は乱数発生手段９３３により乱数Rを発生させ、
情報記憶手段９２５に乱数Rを記憶させ、DVD情報管理手段９３５により
料金情報１１０３を得て、DVD再生装置９００に乱数Rと料金情報１１０３とを送信する
1203
DVD再生装置９００は乱数Rと料金情報１１０３を受信し、乱数Rは情報記憶手段９０５に記憶させ、
料金情報１１０３は情報表示手段９０３に表示し、利用者にクレジットカード番号を入力させる
1204
送信データ暗号化手段９１２において、情報記憶手段９０５に記憶しておいたRと、
DVD駆動手段９０７によってDVD９０６のメディア活用情報から得た
料金サーバ公開鍵ＰＳとを用いて、利用者が入力したクレジットカード番号Nを暗号化する
1205
DVD再生装置９００は暗号化したクレジットカード番号を
料金サーバ９２０に対して送信する
1206
料金サーバ９２０は暗号化したクレジットカード番号を受信し、
情報記憶手段９２５に記憶しておいたRと、ＩＣカード駆動手段９３０によってＩＣカード９２９から得た
料金サーバ秘密鍵ＳＳとを用いて受信データ復号化手段によってクレジットカード番号Nを復号化する
1207
クレジットカード番号送信終了

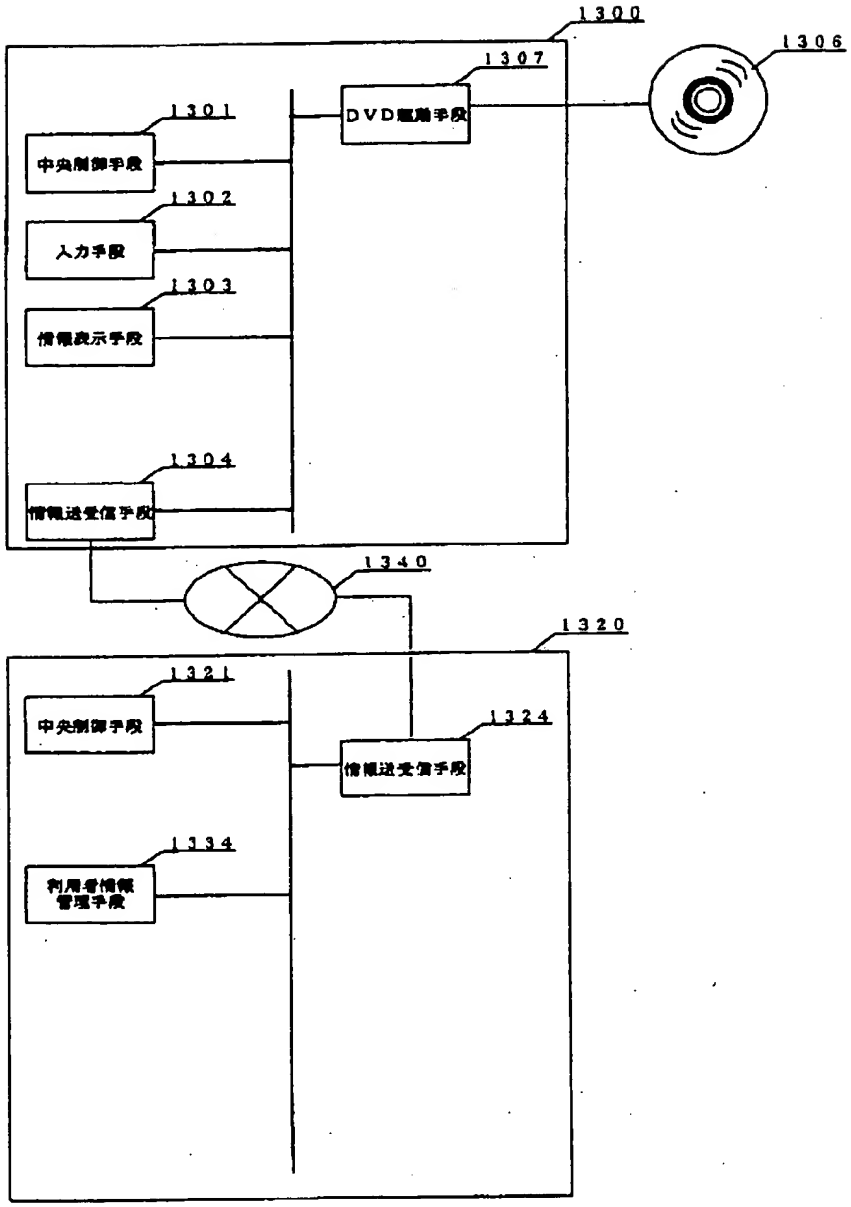
【図１５】


1500
利用者情報
1501
1502
1504
タイトル情報
発行番号情報
使用量累計

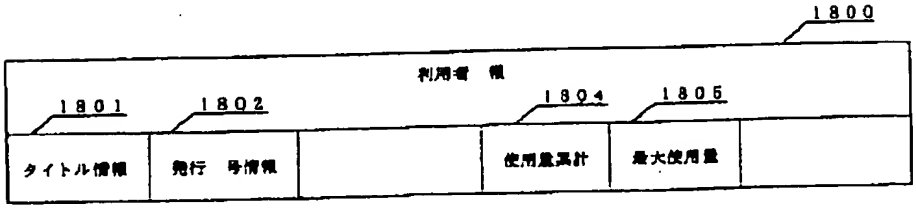
【図１７】


1700
利用者情報
1701
1702
1707
1704
タイトル情報
発行番号情報
映画作品名
使用量累計

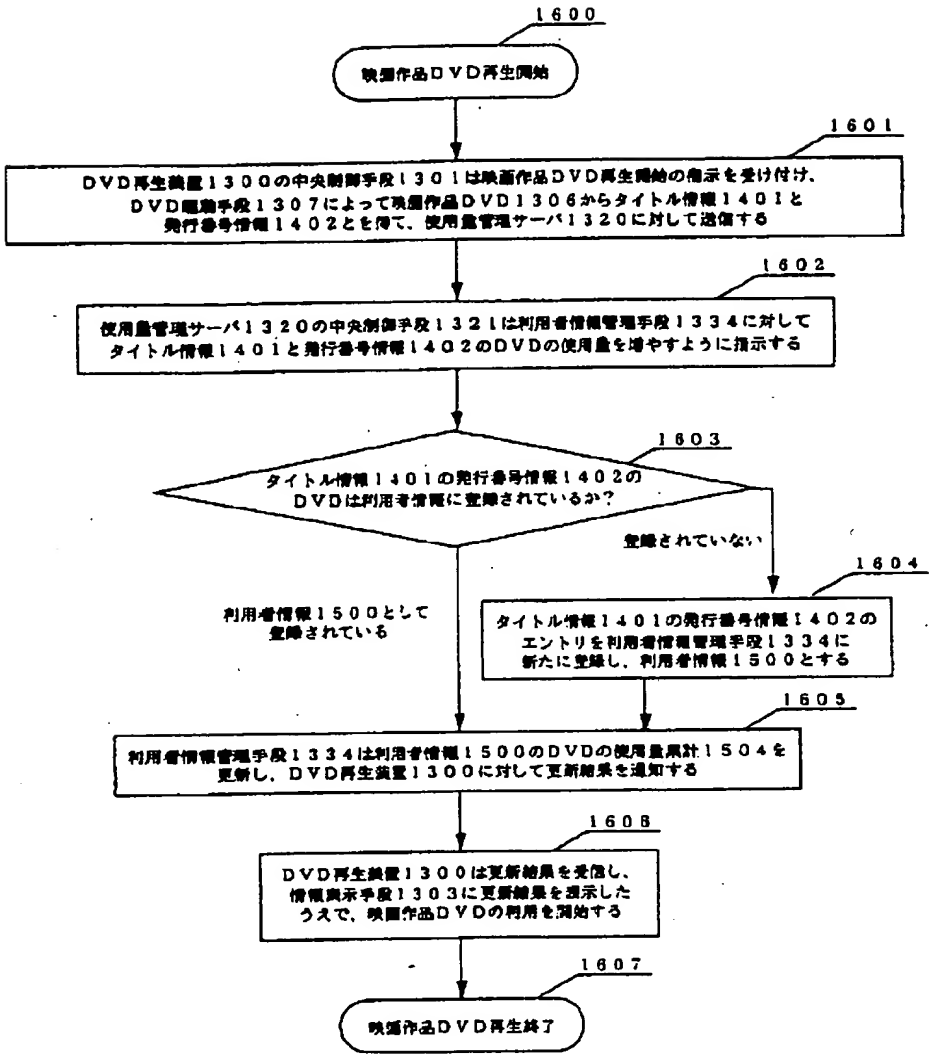
【図１３】


1300
1306
1307
DVD記録手段
1301
中央制御手段
1302
入力手段
1303
情報表示手段
1304
情報送受信手段
1340
1320
1321
中央制御手段
1324
情報送受信手段
1334
利用者情報
管理手段

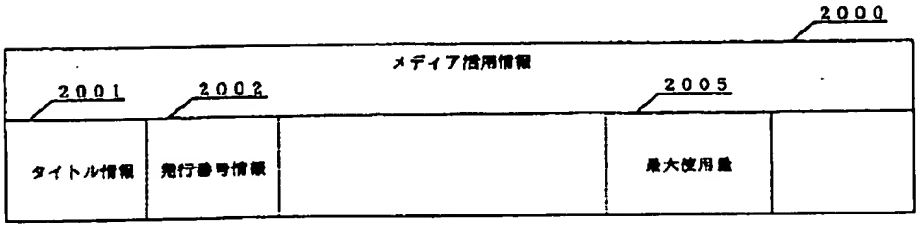
【図１８】


1800
利用者 情報
1801
1802
1804
1805
タイトル情報
発行 号情報
使用量累計
最大使用量

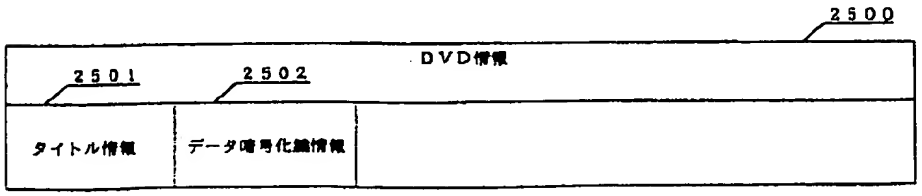
【図１６】


1600
映画作品ＤＶＤ再生開始
1601
ＤＶＤ再生装置１３００の中央制御手段１３０１は映画作品ＤＶＤ再生開始の指示を受け付け、
ＤＶＤ読取手段１３０７によって映画作品ＤＶＤ１３０６からタイトル情報１４０１と
発行番号情報１４０２とを得て、使用量管理サーバ１３２０に対して送信する
1602
使用量管理サーバ１３２０の中央制御手段１３２１は利用者情報管理手段１３３４に対して
タイトル情報１４０１と発行番号情報１４０２のＤＶＤの使用量を増やすように指示する
1603
タイトル情報１４０１の発行番号情報１４０２の
ＤＶＤは利用者情報に登録されているか？
登録されていない
利用者情報１５００として
登録されている
1604
タイトル情報１４０１の発行番号情報１４０２の
エントリを利用者情報管理手段１３３４に
新たに登録し、利用者情報１５００とする
1605
利用者情報管理手段１３３４は利用者情報１５００のＤＶＤの使用量累計１５０４を
更新し、ＤＶＤ再生装置１３００に対して更新結果を通知する
1606
ＤＶＤ再生装置１３００は更新結果を受信し、
情報表示手段１３０３に更新結果を表示した
うえで、映画作品ＤＶＤの利用を開始する
1607
映画作品ＤＶＤ再生終了

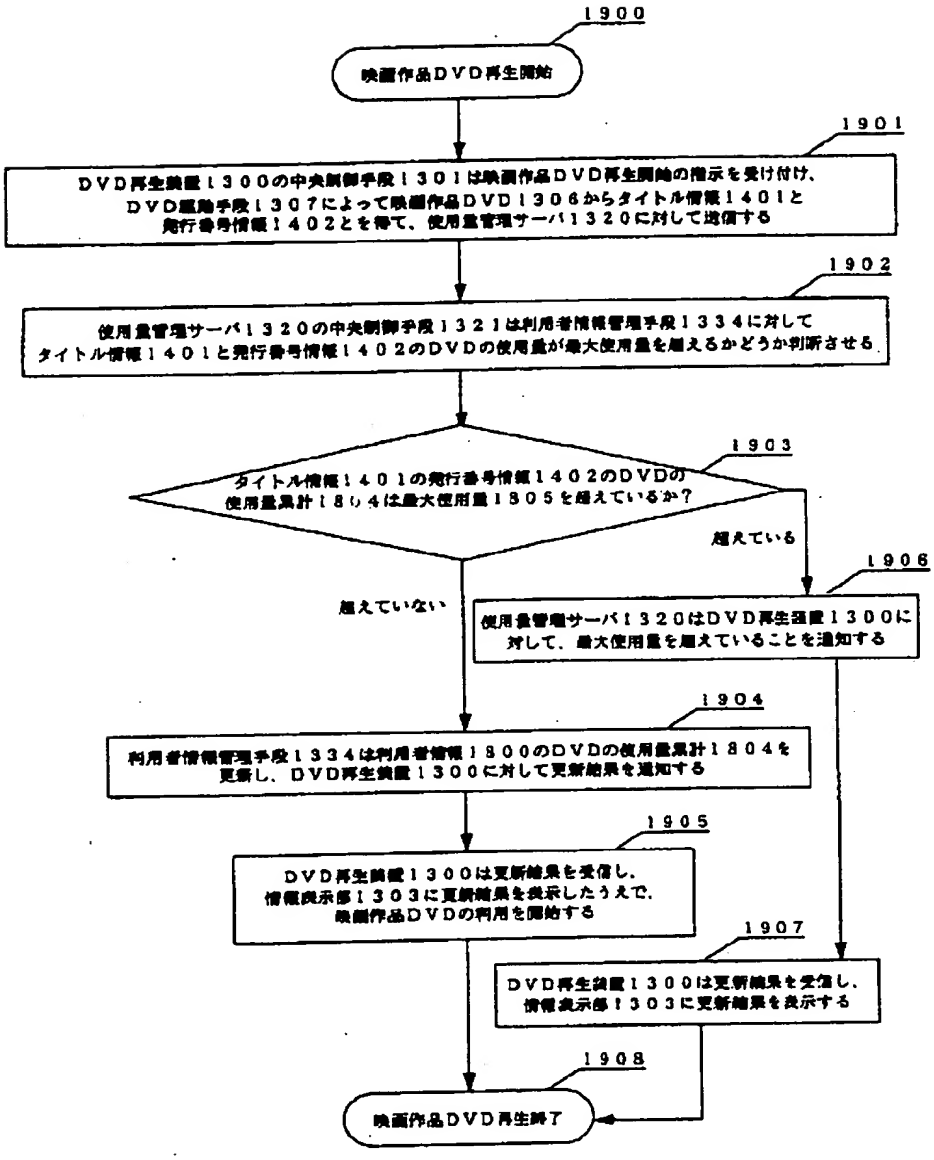
【図２０】


2000
メディア管理情報
2001
2002
2005
タイトル情報
発行番号情報
最大使用量

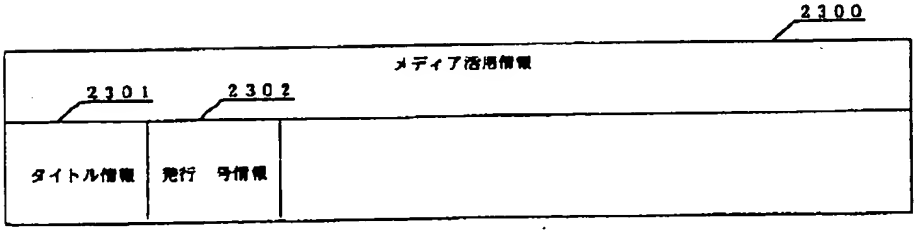
【図２５】


2500
ＤＶＤ情報
2501
2502
タイトル情報
データ暗号化鍵情報

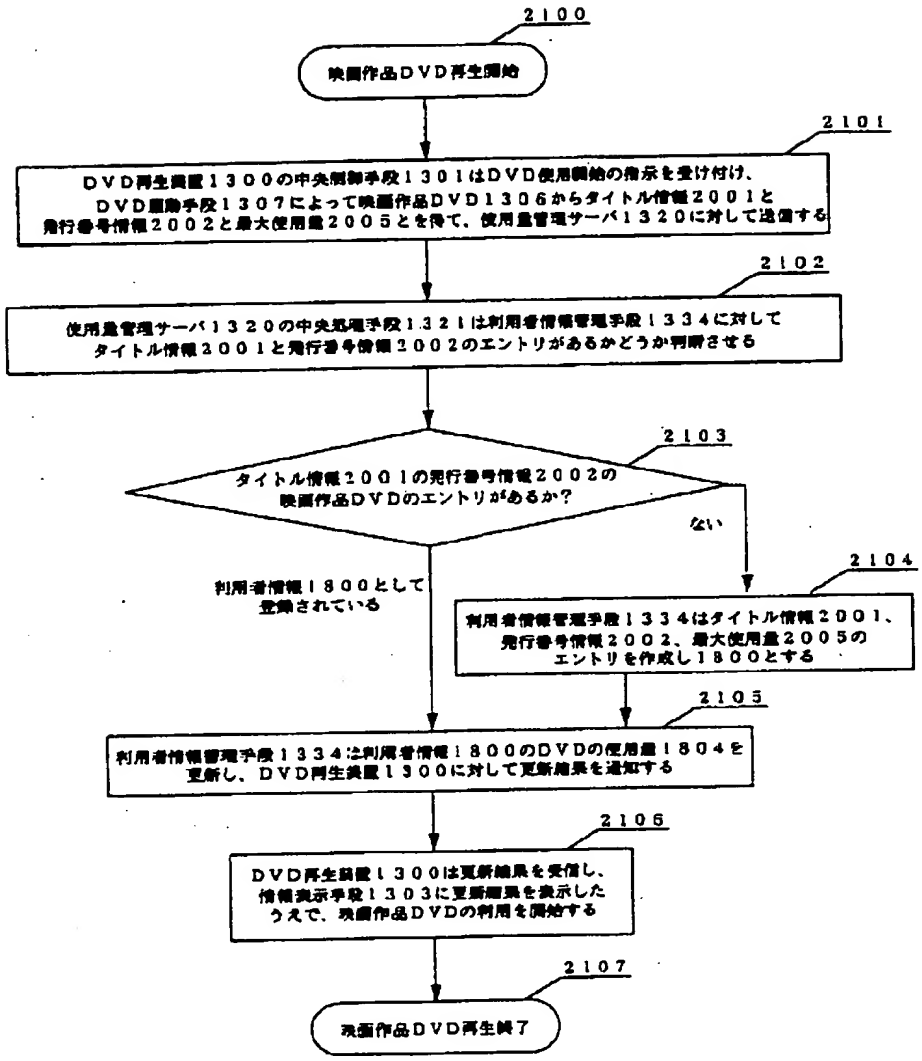
【図１９】


1900
映画作品ＤＶＤ再生開始
1901
ＤＶＤ再生装置１３００の中央制御手段１３０１は映画作品ＤＶＤ再生開始の指示を受け付け、
ＤＶＤ駆動手段１３０７によって映画作品ＤＶＤ１３０６からタイトル情報１４０１と
発行番号情報１４０２とを得て、使用量管理サーバ１３２０に対して送信する
1902
使用量管理サーバ１３２０の中央制御手段１３２１は利用者情報管理手段１３３４に対して
タイトル情報１４０１と発行番号情報１４０２のＤＶＤの使用量が最大使用量を超えるかどうか判断させる
1903
タイトル情報１４０１の発行番号情報１４０２のＤＶＤの
使用量累計１８０４は最大使用量１８０５を超えているか？
超えている
超えていない
1906
使用量管理サーバ１３２０はＤＶＤ再生装置１３００に
対して、最大使用量を超えていることを通知する
1904
利用者情報管理手段１３３４は利用者情報１８００のＤＶＤの使用量累計１８０４を
更新し、ＤＶＤ再生装置１３００に対して更新結果を通知する
1905
ＤＶＤ再生装置１３００は更新結果を受信し、
情報表示部１３０３に更新結果を表示したうえで、
映画作品ＤＶＤの利用を開始する
1907
ＤＶＤ再生装置１３００は更新結果を受信し、
情報表示部１３０３に更新結果を表示する
1908
映画作品ＤＶＤ再生終了

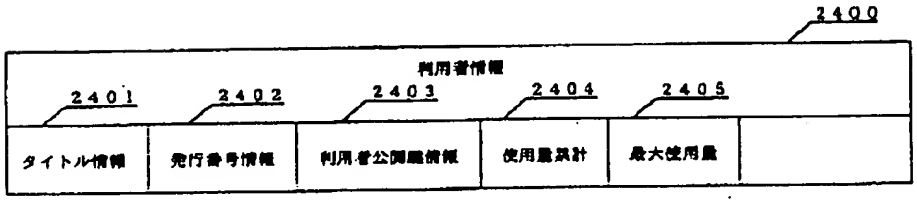
【図２３】


2300
メディア活用情報
2301
2302
タイトル情報
発行　号情報

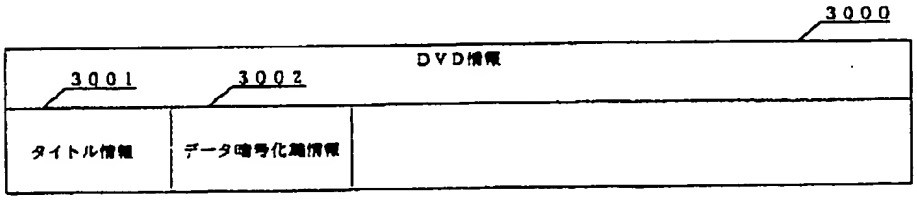
【図２１】


2100
映画作品DVD再生開始
2101
DVD再生装置1300の中央制御手段1301はDVD使用開始の指示を受け付け、
DVD通信手段1307によって映画作品DVD1306からタイトル情報2001と
発行番号情報2002と最大使用量2005とを得て、使用量管理サーバ1320に対して送信する
2102
使用量管理サーバ1320の中央処理手段1321は利用者情報管理手段1334に対して
タイトル情報2001と発行番号情報2002のエントリがあるかどうか判断させる
2103
タイトル情報2001の発行番号情報2002の
映画作品DVDのエントリがあるか?
ない
利用者情報1800として
登録されている
2104
利用者情報管理手段1334はタイトル情報2001、
発行番号情報2002、最大使用量2005の
エントリを作成し1800とする
2105
利用者情報管理手段1334は利用者情報1800のDVDの使用量1804を
更新し、DVD再生装置1300に対して更新結果を通知する
2106
DVD再生装置1300は更新結果を受信し、
情報表示手段1303に更新結果を表示した
うえで、映画作品DVDの利用を開始する
2107
映画作品DVD再生終了

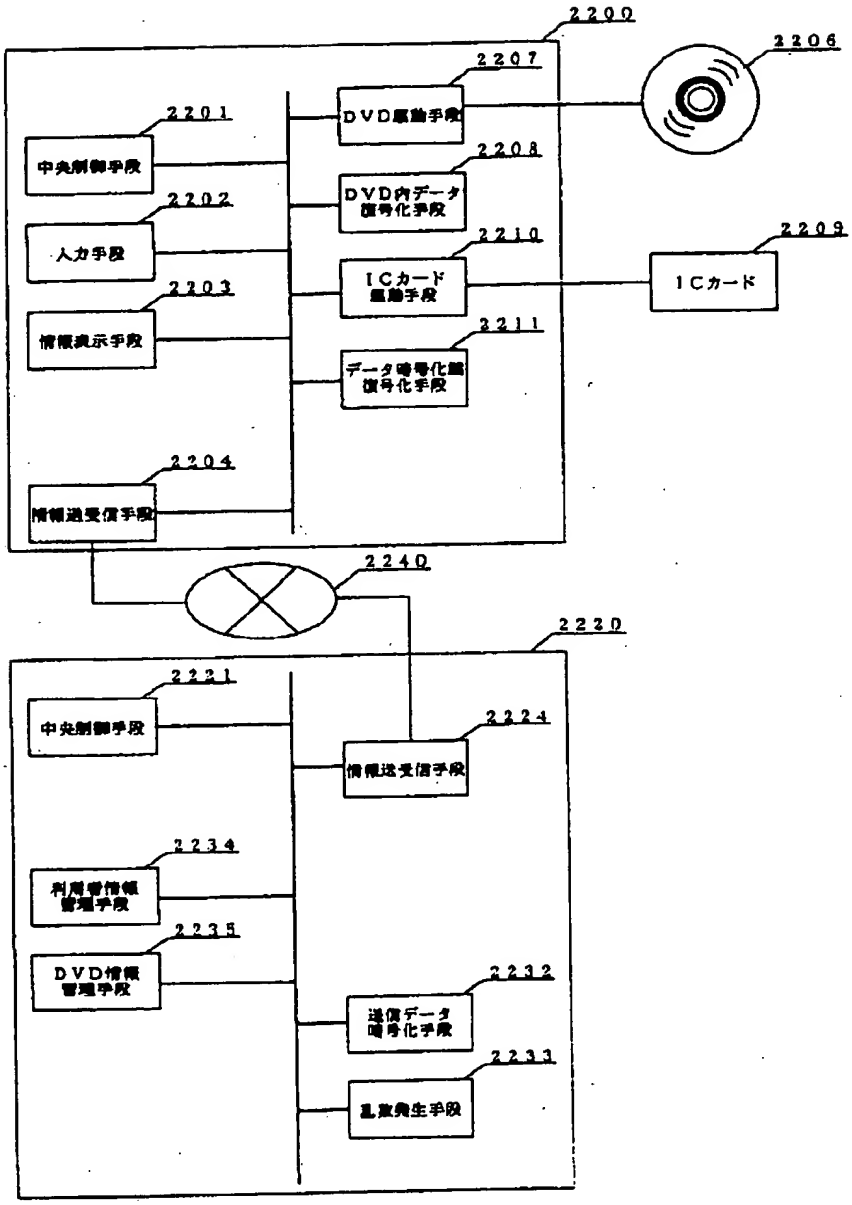
【図２４】


2400
利用者情報
2401
2402
2403
2404
2405
タイトル情報
発行番号情報
利用者公開鍵情報
使用量累計
最大使用量

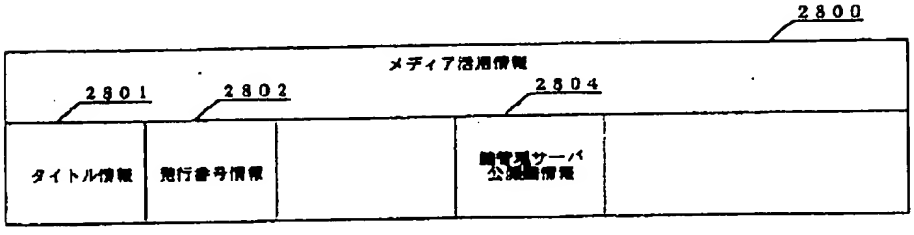
【図３０】


3000
DVD情報
3001
3002
タイトル情報
データ暗号化鍵情報

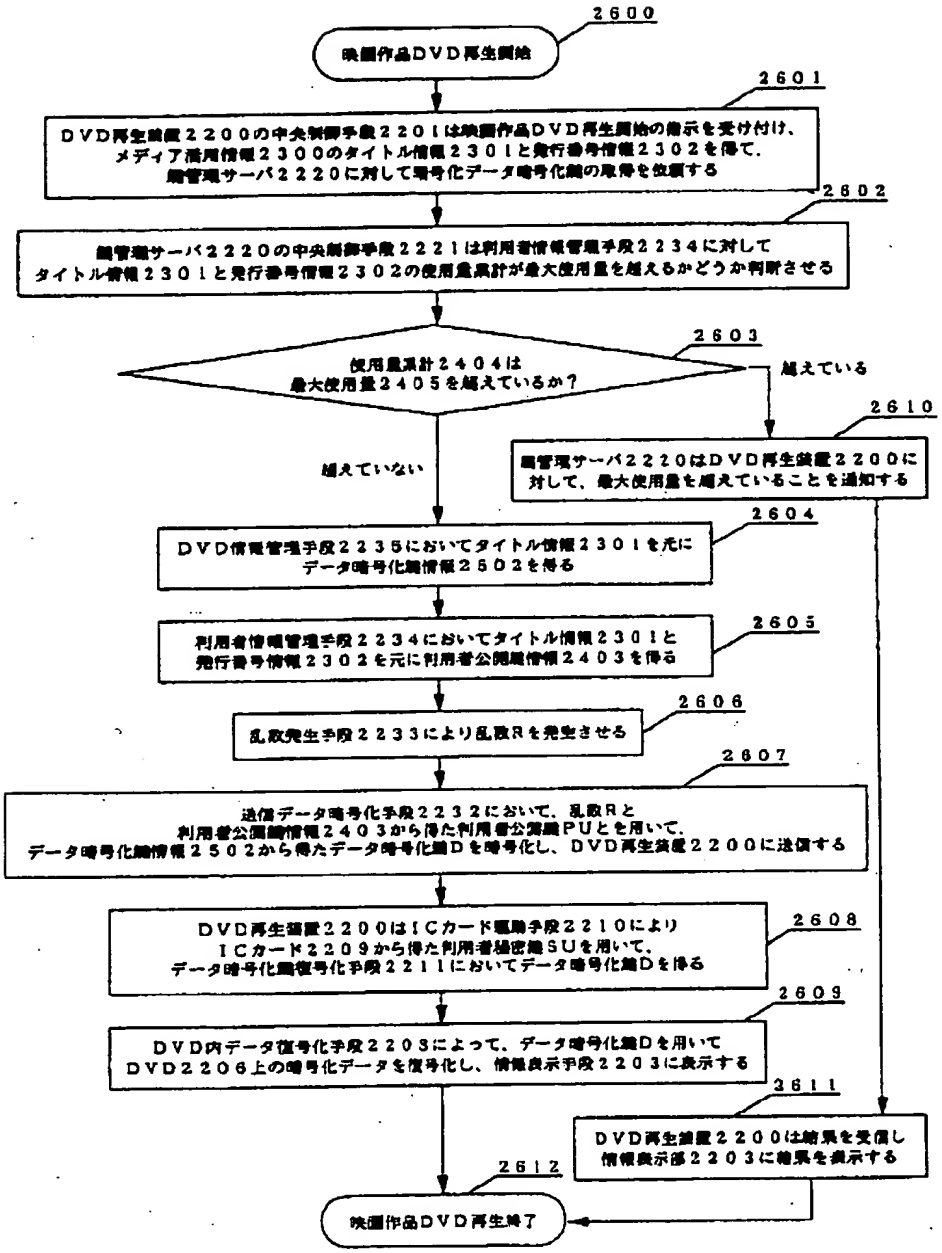
【図２２】


2200
2206
2207
DVD駆動手段
2201
中央制御手段
2208
DVD内データ暗号化手段
2202
入力手段
2210
2209
ICカード
ICカード駆動手段
2203
情報表示手段
2211
データ暗号化鍵復号化手段
2204
情報送受信手段
2240
2220
2221
中央制御手段
2224
情報送受信手段
2234
利用者情報管理手段
2235
DVD情報管理手段
2232
送信データ暗号化手段
2233
乱数発生手段

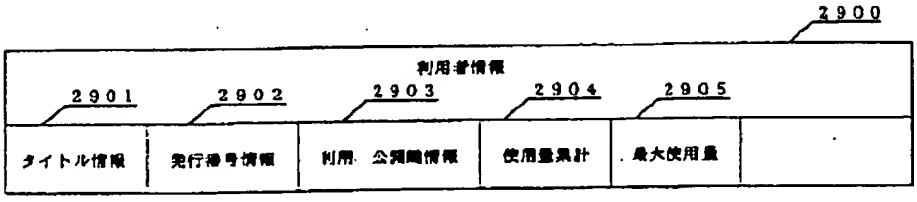
【図２８】


2800
メディア活用情報
2801
2802
2804
タイトル情報
発行番号情報
暗号鍵サーバ公開鍵情報

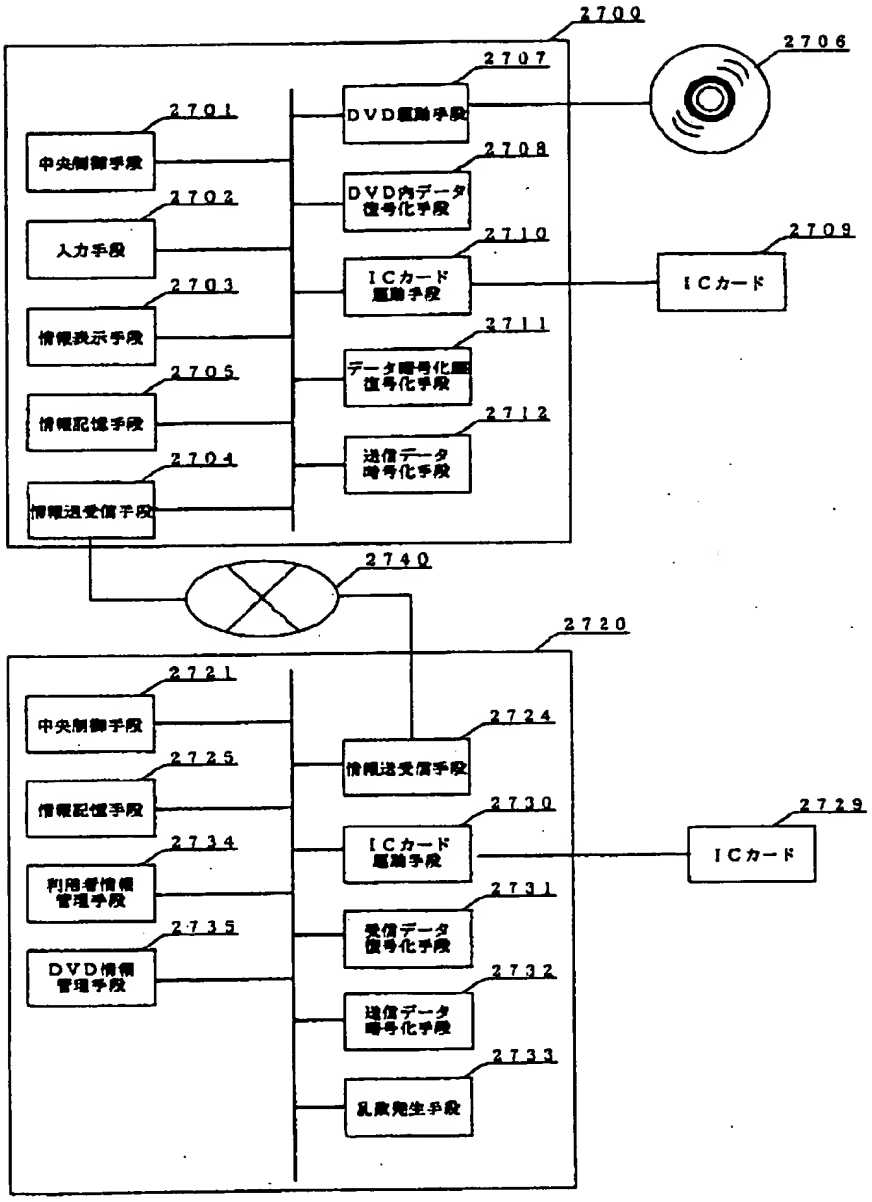
【図２６】


2600
映画作品ＤＶＤ再生開始
2601
ＤＶＤ再生装置２２００の中央制御手段２２０１は映画作品ＤＶＤ再生開始の指示を受け付け、
メディア識別情報２３００のタイトル情報２３０１と発行番号情報２３０２を得て、
課管理サーバ２２２０に対して暗号化データ暗号化鍵の取得を依頼する
2602
課管理サーバ２２２０の中央制御手段２２２１は利用者情報管理手段２２３４に対して
タイトル情報２３０１と発行番号情報２３０２の使用量累計が最大使用量を超えるかどうか判断させる
2603
使用量累計２４０４は
最大使用量２４０５を超えているか？
超えている
超えていない
2610
課管理サーバ２２２０はＤＶＤ再生装置２２００に
対して、最大使用量を超えていることを通知する
2604
ＤＶＤ情報管理手段２２３５においてタイトル情報２３０１を元に
データ暗号化鍵情報２５０２を得る
2605
利用者情報管理手段２２３４においてタイトル情報２３０１と
発行番号情報２３０２を元に利用者公開鍵情報２４０３を得る
2606
乱数発生手段２２３３により乱数Ｒを発生させる
2607
送信データ暗号化手段２２３２において、乱数Ｒと
利用者公開鍵情報２４０３から得た利用者公開鍵ＰＵとを用いて、
データ暗号化鍵情報２５０２から得たデータ暗号化鍵Ｄを暗号化し、ＤＶＤ再生装置２２００に送信する
2608
ＤＶＤ再生装置２２００はＩＣカード駆動手段２２１０により
ＩＣカード２２０９から得た利用者秘密鍵ＳＵを用いて、
データ暗号化鍵復号化手段２２１１においてデータ暗号化鍵Ｄを得る
2609
ＤＶＤ内データ復号化手段２２０３によって、データ暗号化鍵Ｄを用いて
ＤＶＤ２２０６上の暗号化データを復号化し、情報表示手段２２０３に表示する
3611
ＤＶＤ再生装置２２００は結果を受信し
情報表示部２２０３に結果を表示する
2612
映画作品ＤＶＤ再生終了

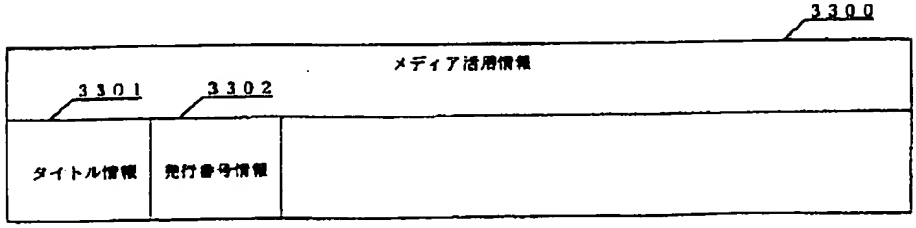
【図２９】


2900
利用者情報
2901
2902
2903
2904
2905
タイトル情報
発行番号情報
利用・公開鍵情報
使用量累計
最大使用量

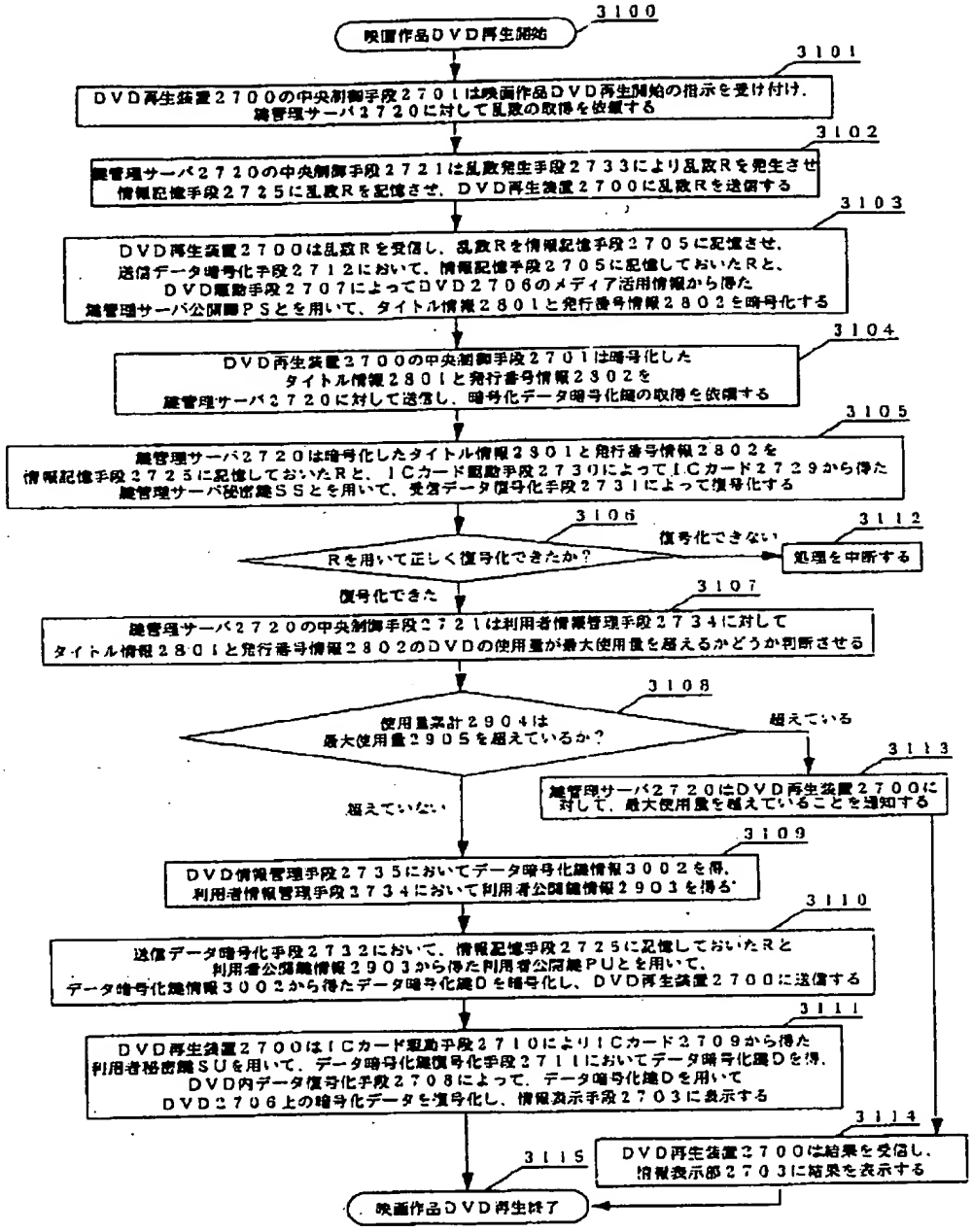
【図２７】


2700
2706
2707
2701
DVD駆動手段
中央制御手段
2708
DVD内データ
復号化手段
2702
入力手段
2709
2710
ICカード
駆動手段
ICカード
2703
情報表示手段
2711
データ暗号化
復号化手段
2705
情報記憶手段
2712
送信データ
暗号化手段
2704
情報送受信手段
2740
2720
2721
中央制御手段
2724
情報送受信手段
2725
情報記憶手段
2729
2730
ICカード
駆動手段
ICカード
2734
利用者情報
管理手段
2731
受信データ
復号化手段
2735
DVD情報
管理手段
2732
送信データ
暗号化手段
2733
乱数発生手段

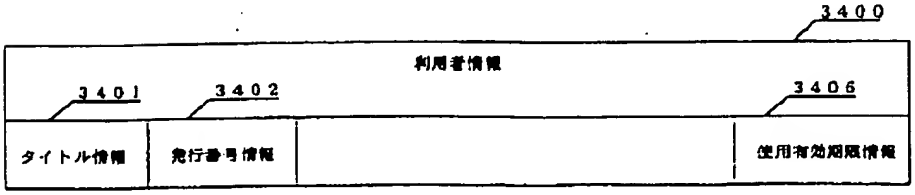
【図３３】


3300
メディア活用情報
3301
3302
タイトル情報
発行番号情報

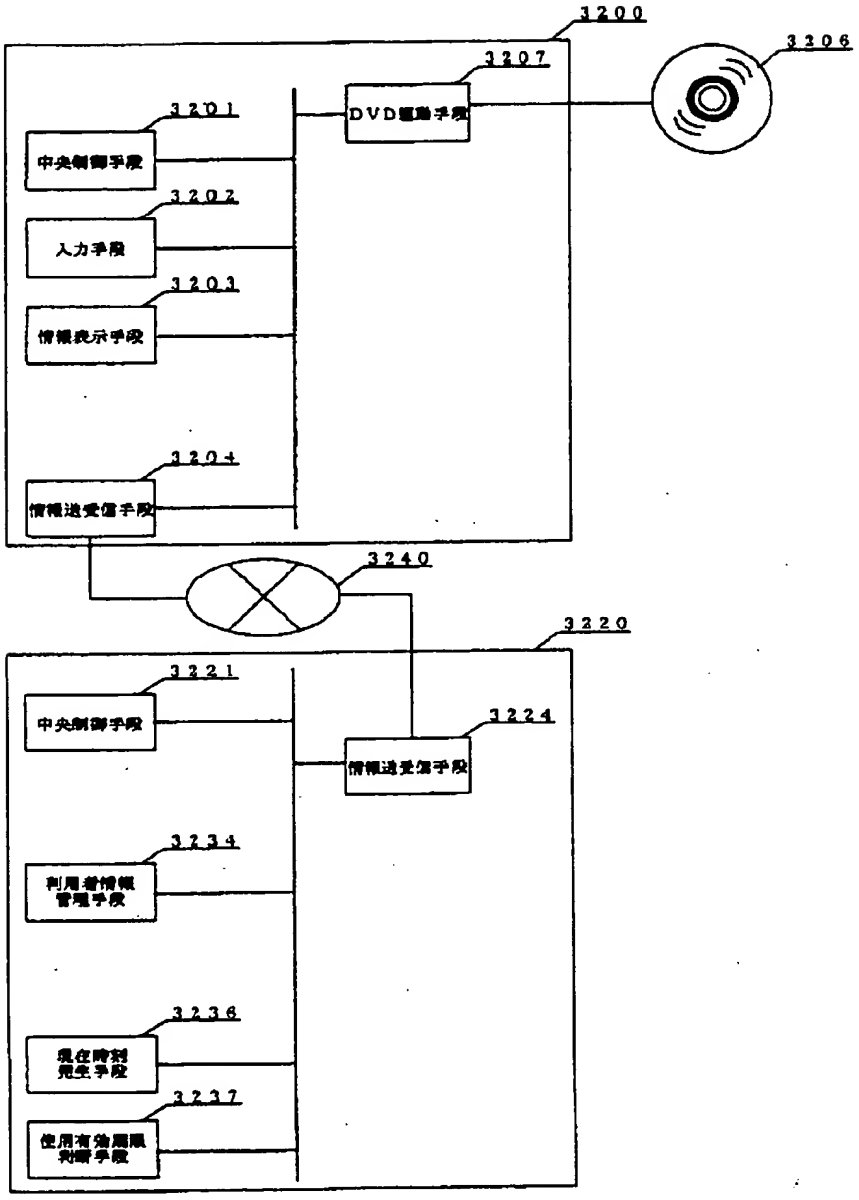
【図３１】


3100
映画作品ＤＶＤ再生開始
3101
ＤＶＤ再生装置２７００の中央制御手段２７０１は映画作品ＤＶＤ再生開始の指示を受け付け、
鍵管理サーバ２７２０に対して乱数の取得を依頼する
3102
鍵管理サーバ２７２０の中央制御手段２７２１は乱数発生手段２７３３により乱数Ｒを発生させ
情報記憶手段２７２５に乱数Ｒを記憶させ、ＤＶＤ再生装置２７００に乱数Ｒを送信する
3103
ＤＶＤ再生装置２７００は乱数Ｒを受信し、乱数Ｒを情報記憶手段２７０５に記憶させ、
送信データ暗号化手段２７１２において、情報記憶手段２７０５に記憶しておいたＲと、
ＤＶＤ駆動手段２７０７によってＤＶＤ２７０６のメディア活用情報から得た
鍵管理サーバ公開鍵ＰＳとを用いて、タイトル情報２８０１と発行番号情報２８０２を暗号化する
3104
ＤＶＤ再生装置２７００の中央制御手段２７０１は暗号化した
タイトル情報２８０１と発行番号情報２３０２を
鍵管理サーバ２７２０に対して送信し、暗号化データ暗号化鍵の取得を依頼する
3105
鍵管理サーバ２７２０は暗号化したタイトル情報２９０１と発行番号情報２８０２を
情報記憶手段２７２５に記憶しておいたＲと、ＩＣカード駆動手段２７３０によってＩＣカード２７２９から得た
鍵管理サーバ秘密鍵ＳＳとを用いて、受信データ復号化手段２７３１によって復号化する
3106
Ｒを用いて正しく復号化できたか？
復号化できない
3112
処理を中断する
復号化できた
3107
鍵管理サーバ２７２０の中央制御手段２７２１は利用者情報管理手段２７３４に対して
タイトル情報２８０１と発行番号情報２８０２のＤＶＤの使用量が最大使用量を超えるかどうか判断させる
3108
使用量累計２９０４は
最大使用量２９０５を超えているか？
超えている
3113
鍵管理サーバ２７２０はＤＶＤ再生装置２７００に
対して、最大使用量を超えていることを通知する
超えていない
3109
ＤＶＤ情報管理手段２７３５においてデータ暗号化鍵情報３００２を得、
利用者情報管理手段２７３４において利用者公開鍵情報２９０３を得る
3110
送信データ暗号化手段２７３２において、情報記憶手段２７２５に記憶しておいたＲと
利用者公開鍵情報２９０３から得た利用者公開鍵ＰＵとを用いて、
データ暗号化鍵情報３００２から得たデータ暗号化鍵Ｄを暗号化し、ＤＶＤ再生装置２７００に送信する
3111
ＤＶＤ再生装置２７００はＩＣカード駆動手段２７１０によりＩＣカード２７０９から得た
利用者秘密鍵ＳＵを用いて、データ暗号化鍵復号化手段２７１１においてデータ暗号化鍵Ｄを得、
ＤＶＤ内データ復号化手段２７０８によって、データ暗号化鍵Ｄを用いて
ＤＶＤ２７０６上の暗号化データを復号化し、情報表示手段２７０３に表示する
3114
ＤＶＤ再生装置２７００は結果を受信し、
情報表示部２７０３に結果を表示する
3115
映画作品ＤＶＤ再生終了

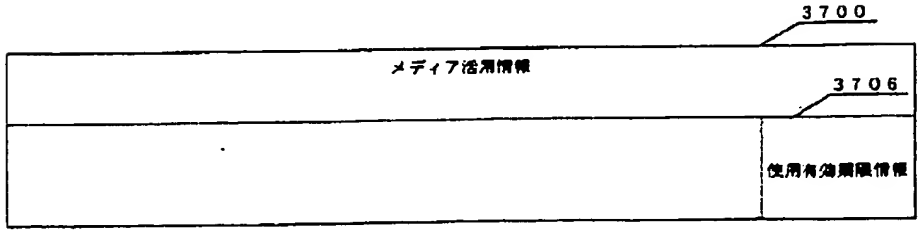
【図３４】


3400
利用者情報
3401
3402
3406
タイトル情報
発行番号情報
使用有効期限情報

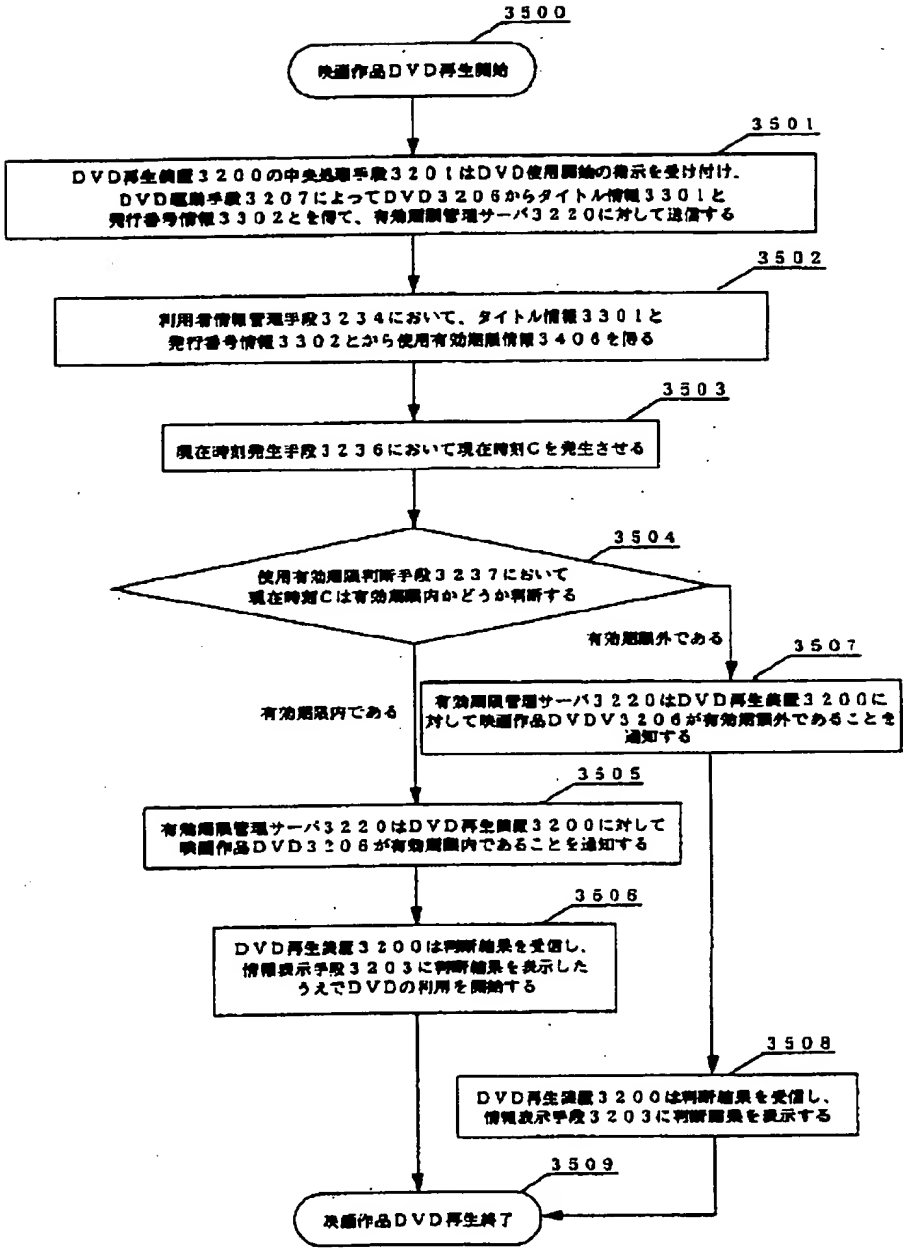
【図３２】


3200
3206
3207
DVD駆動手段
3201
中央制御手段
3202
入力手段
3203
情報表示手段
3204
情報送受信手段
3240
3220
3221
中央制御手段
3224
情報送受信手段
3234
利用者情報管理手段
3236
現在時刻発生手段
3237
使用有効期限判断手段

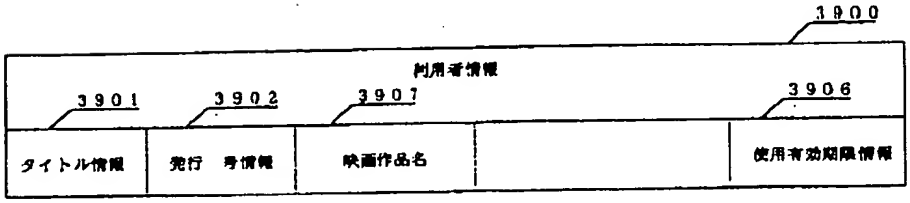
【図３７】


3700
メディア活用情報
3706
使用有効期限情報

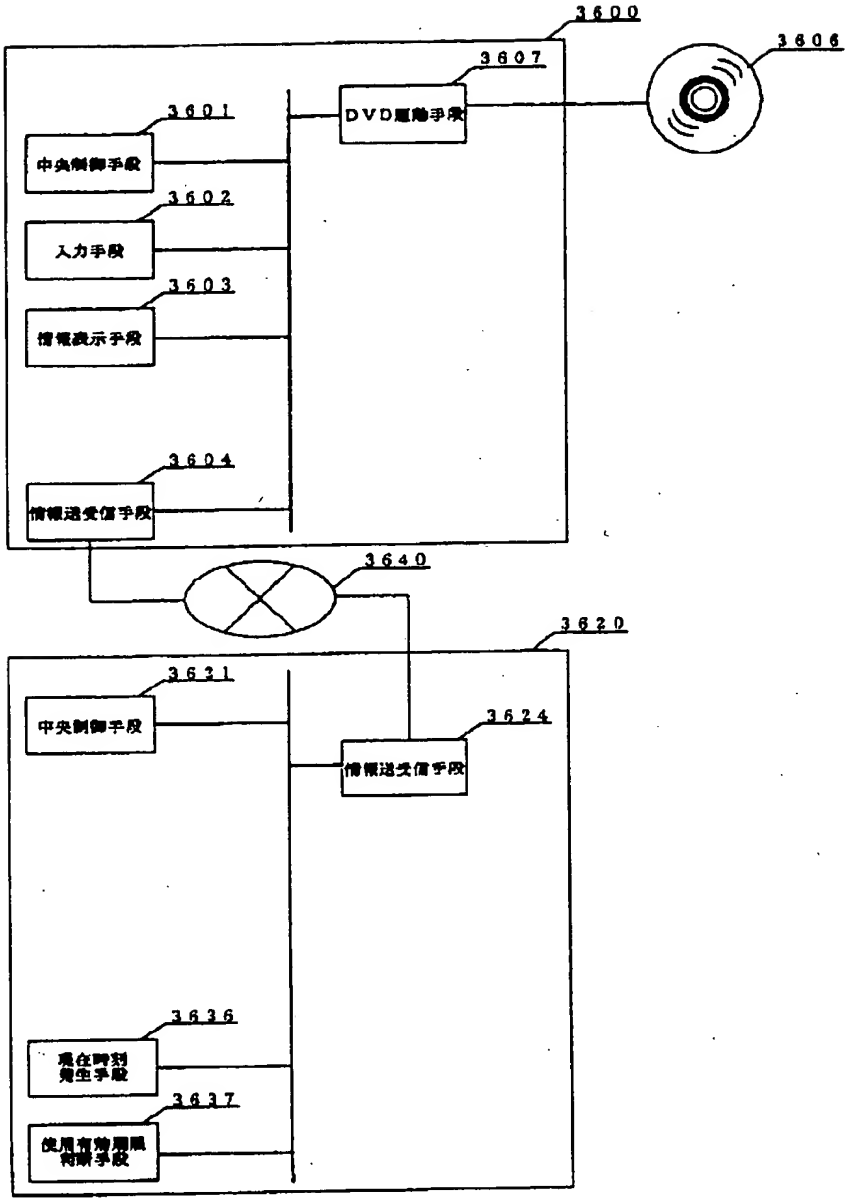
【図３５】


3500
映画作品ＤＶＤ再生開始
3501
ＤＶＤ再生装置３２００の中央処理手段３２０１はＤＶＤ使用開始の指示を受け付け、
ＤＶＤ駆動手段３２０７によってＤＶＤ３２０６からタイトル情報３３０１と
発行番号情報３３０２とを得て、有効期限管理サーバ３２２０に対して送信する
3502
利用者情報管理手段３２３４において、タイトル情報３３０１と
発行番号情報３３０２とから使用有効期限情報３４０６を得る
3503
現在時刻発生手段３２３６において現在時刻Ｃを発生させる
3504
使用有効期限判断手段３２３７において
現在時刻Ｃは有効期限内かどうか判断する
有効期限外である
有効期限内である
3507
有効期限管理サーバ３２２０はＤＶＤ再生装置３２００に
対して映画作品ＤＶＤＶ３２０６が有効期限外であることを
通知する
3505
有効期限管理サーバ３２２０はＤＶＤ再生装置３２００に対して
映画作品ＤＶＤ３２０６が有効期限内であることを通知する
3506
ＤＶＤ再生装置３２００は判断結果を受信し、
情報表示手段３２０３に判断結果を表示した
うえでＤＶＤの利用を開始する
3508
ＤＶＤ再生装置３２００は判断結果を受信し、
情報表示手段３２０３に判断結果を表示する
3509
映画作品ＤＶＤ再生終了

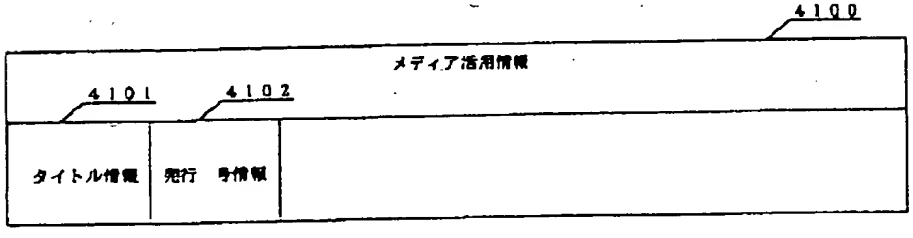
【図３９】


3900
利用者情報
3901
3902
3907
3906
タイトル情報
発行　号情報
映画作品名
使用有効期限情報

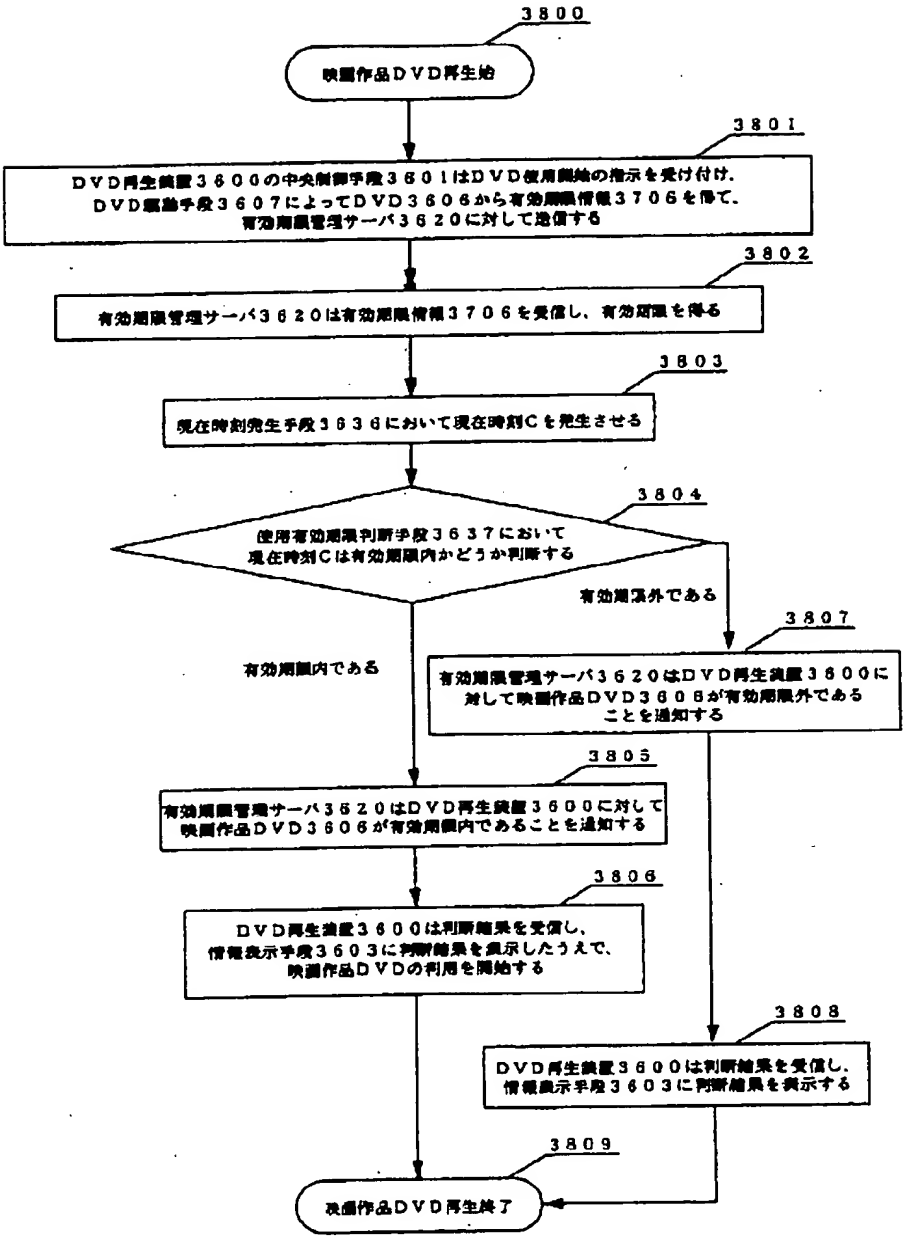
【図３６】


3600
3606
3607
DVD駆動手段
3601
中央制御手段
3602
入力手段
3603
情報表示手段
3604
情報送受信手段
3640
3620
3631
中央制御手段
3624
情報送受信手段
3636
現在時刻発生手段
3637
使用有効期限判断手段

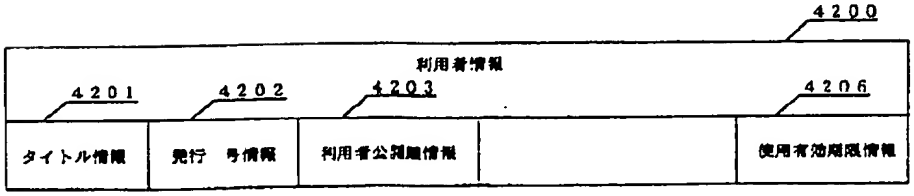
【図４１】


4100
メディア活用情報
4101
4102
タイトル情報
発行　号情報

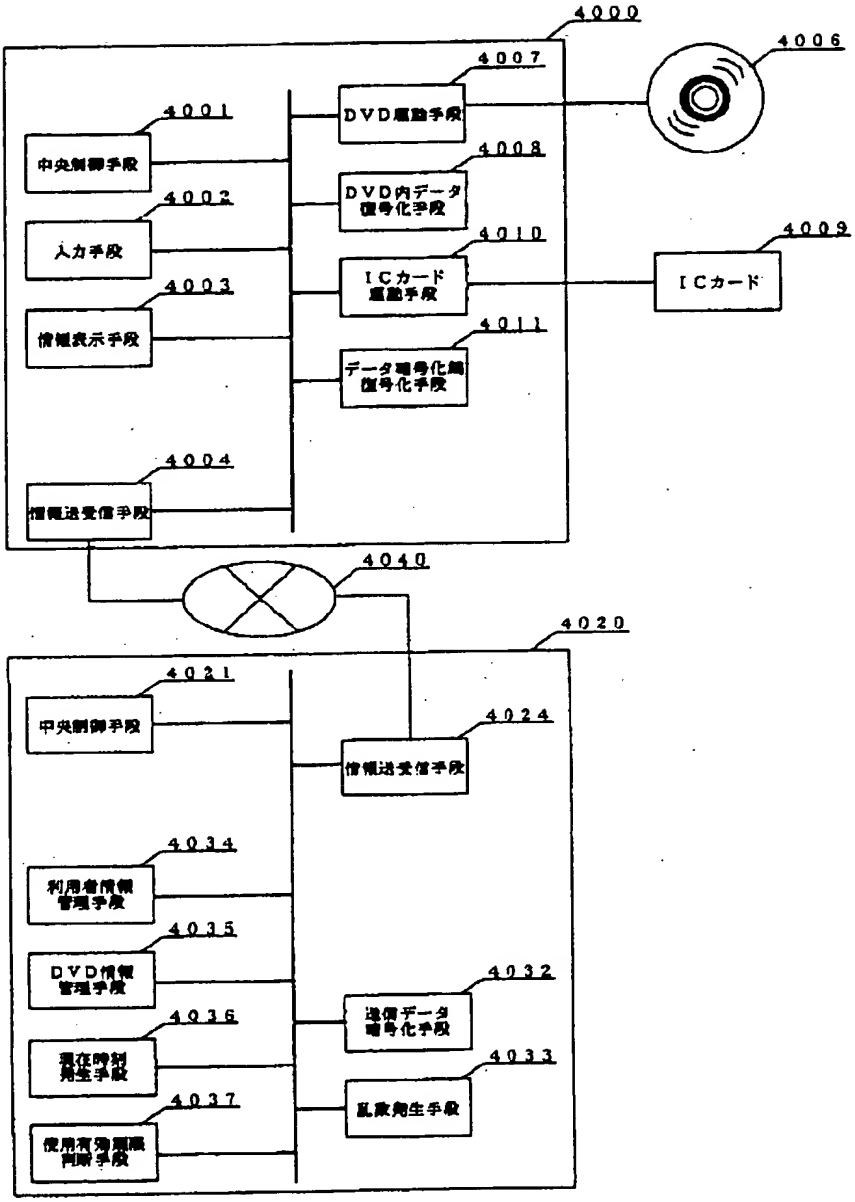
【図３８】


3800
映画作品ＤＶＤ再生始
3801
ＤＶＤ再生装置３６００の中央制御手段３６０１はＤＶＤ使用開始の指示を受け付け、
ＤＶＤ駆動手段３６０７によってＤＶＤ３６０６から有効期限情報３７０６を得て、
有効期限管理サーバ３６２０に対して送信する
3802
有効期限管理サーバ３６２０は有効期限情報３７０６を受信し、有効期限を得る
3803
現在時刻発生手段３６３６において現在時刻Ｃを発生させる
3804
使用有効期限判断手段３６３７において
現在時刻Ｃは有効期限内かどうか判断する
有効期限外である
有効期限内である
3807
有効期限管理サーバ３６２０はＤＶＤ再生装置３６００に
対して映画作品ＤＶＤ３６０６が有効期限外である
ことを通知する
3805
有効期限管理サーバ３６２０はＤＶＤ再生装置３６００に対して
映画作品ＤＶＤ３６０６が有効期限内であることを通知する
3806
ＤＶＤ再生装置３６００は判断結果を受信し、
情報表示手段３６０３に判断結果を表示したうえで、
映画作品ＤＶＤの利用を開始する
3808
ＤＶＤ再生装置３６００は判断結果を受信し、
情報表示手段３６０３に判断結果を表示する
3809
映画作品ＤＶＤ再生終了

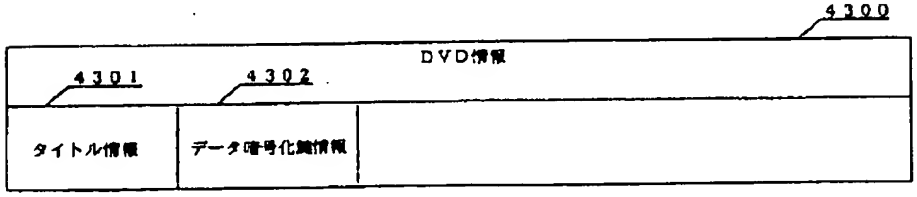
【図４２】


4200
利用者情報
4201
4202
4203
4206
タイトル情報
発行　号情報
利用者公開鍵情報
使用有効期限情報

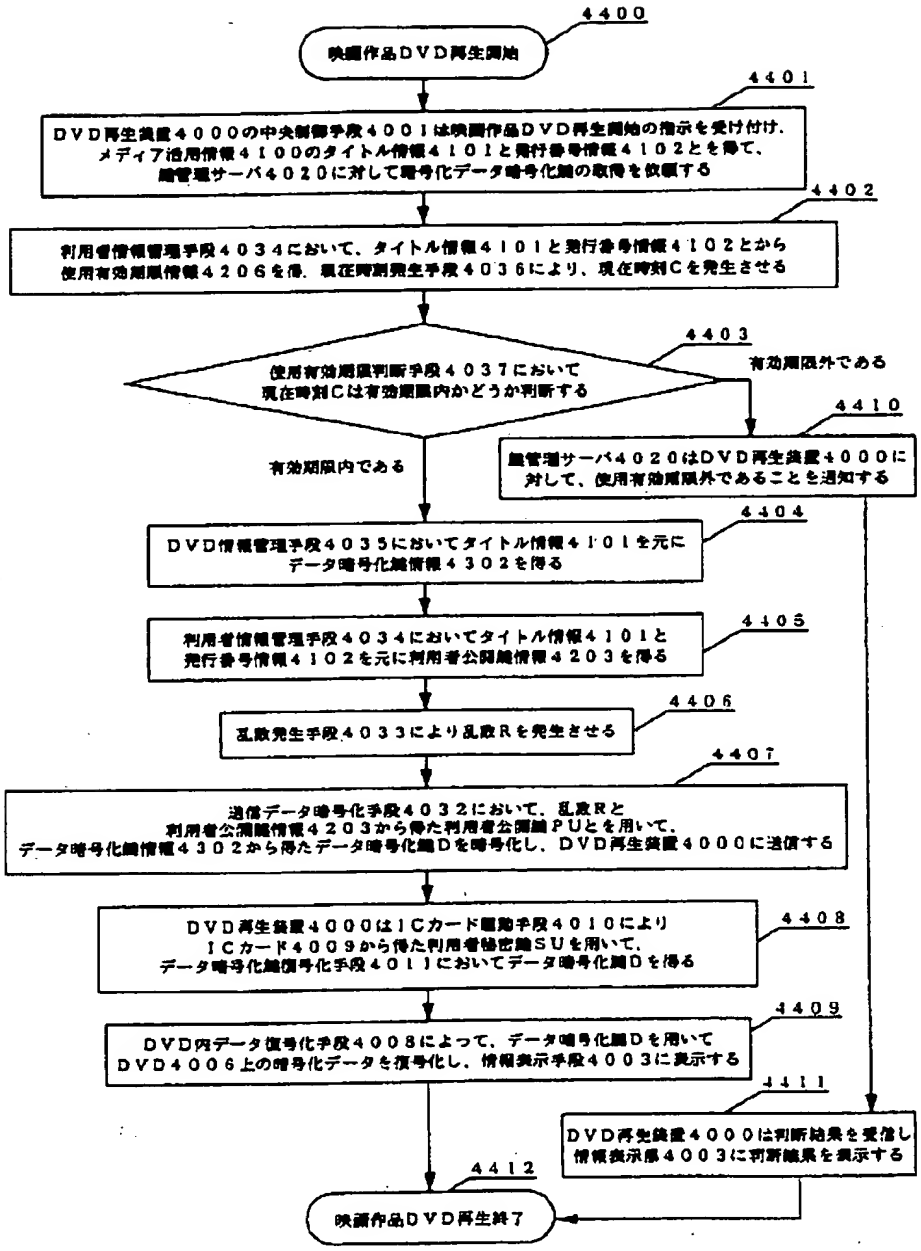
【図４０】


4000
4006
4007
DVD駆動手段
4001
中央制御手段
4008
DVD内データ暗号化手段
4002
入力手段
4010
ICカード駆動手段
4009
ICカード
4003
情報表示手段
4011
データ暗号化鍵暗号化手段
4004
情報送受信手段
4040
4020
4021
中央制御手段
4024
情報送受信手段
4034
利用者情報管理手段
4035
DVD情報管理手段
4032
送信データ暗号化手段
4036
現在時刻発生手段
4033
乱数発生手段
4037
使用有効期限判断手段

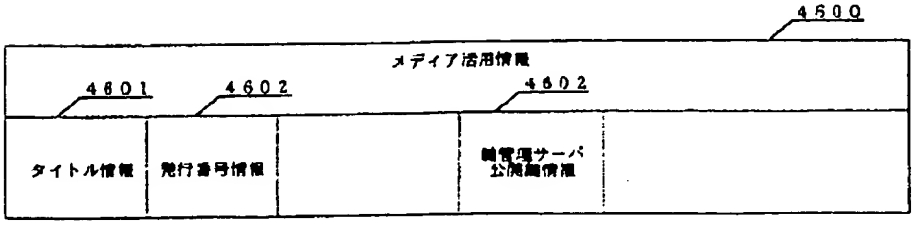
【図４３】


4300
DVD情報
4301
4302
タイトル情報
データ暗号化鍵情報

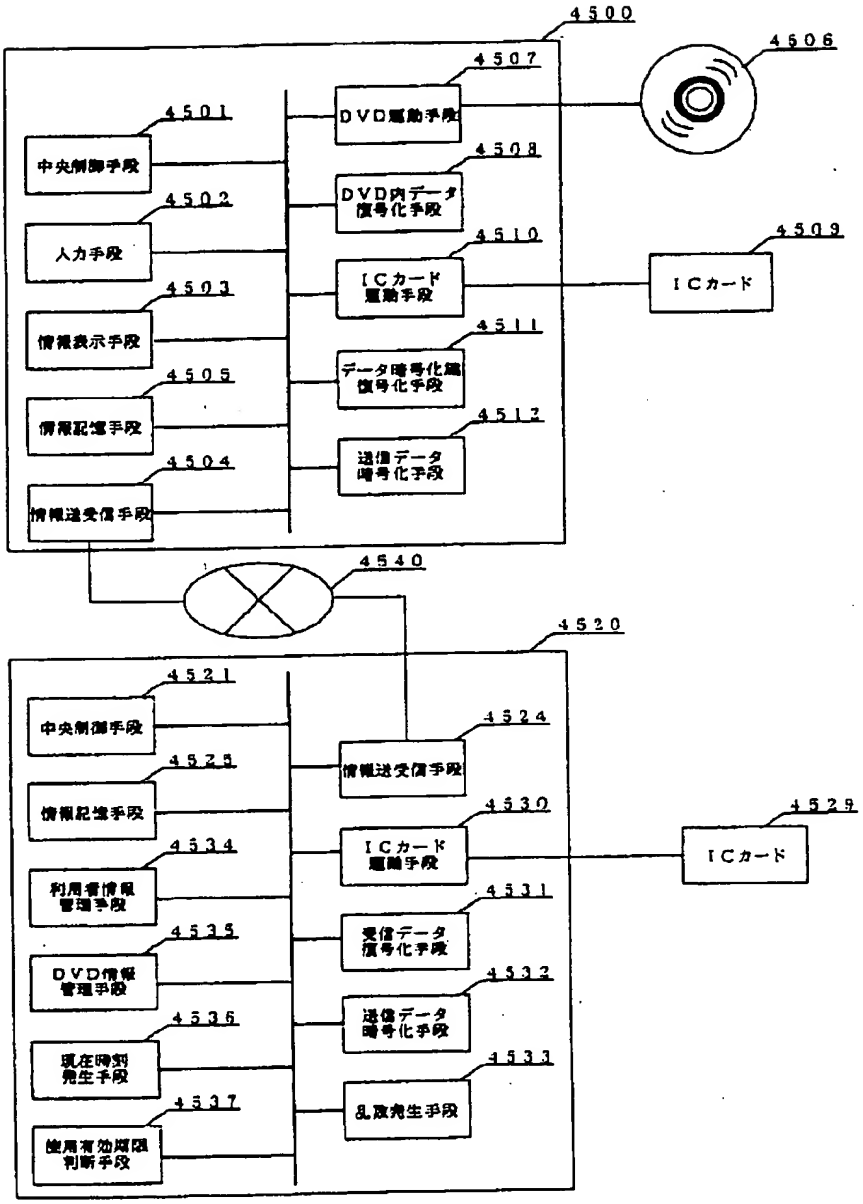
【図４４】


4400
映画作品ＤＶＤ再生開始
4401
ＤＶＤ再生装置４０００の中央制御手段４００１は映画作品ＤＶＤ再生開始の指示を受け付け、
メディア活用情報４１００のタイトル情報４１０１と発行番号情報４１０２とを得て、
鍵管理サーバ４０２０に対して暗号化データ暗号化鍵の取得を依頼する
4402
利用者情報管理手段４０３４において、タイトル情報４１０１と発行番号情報４１０２とから
使用有効期限情報４２０６を得、現在時刻発生手段４０３６により、現在時刻Ｃを発生させる
4403
使用有効期限判断手段４０３７において
現在時刻Ｃは有効期限内かどうか判断する
有効期限外である
4410
鍵管理サーバ４０２０はＤＶＤ再生装置４０００に
対して、使用有効期限外であることを通知する
有効期限内である
4404
ＤＶＤ情報管理手段４０３５においてタイトル情報４１０１を元に
データ暗号化鍵情報４３０２を得る
4405
利用者情報管理手段４０３４においてタイトル情報４１０１と
発行番号情報４１０２を元に利用者公開鍵情報４２０３を得る
4406
乱数発生手段４０３３により乱数Ｒを発生させる
4407
通信データ暗号化手段４０３２において、乱数Ｒと
利用者公開鍵情報４２０３から得た利用者公開鍵ＰＵとを用いて、
データ暗号化鍵情報４３０２から得たデータ暗号化鍵Ｄを暗号化し、ＤＶＤ再生装置４０００に送信する
ＤＶＤ再生装置４０００はＩＣカード開始手段４０１０により
ＩＣカード４００９から得た利用者秘密鍵ＳＵを用いて、
データ暗号化鍵復号化手段４０１１においてデータ暗号化鍵Ｄを得る
4408
4409
ＤＶＤ内データ復号化手段４００８によって、データ暗号化鍵Ｄを用いて
ＤＶＤ４００６上の暗号化データを復号化し、情報表示手段４００３に表示する
4411
ＤＶＤ再生装置４０００は判断結果を受信し
情報表示部４００３に判断結果を表示する
4412
映画作品ＤＶＤ再生終了

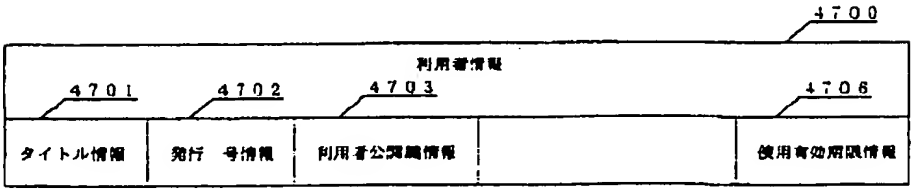
【図４６】


4500
メディア活用情報
4601
4602
4602
タイトル情報
発行番号情報
鍵管理サーバ
公開鍵情報

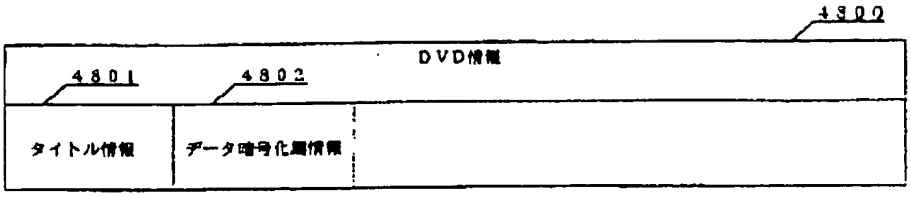
【図４５】


4500
4506
4507
DVD駆動手段
4501
中央制御手段
4508
DVD内データ復号化手段
4502
入力手段
4510
4509
ICカード駆動手段
ICカード
4503
情報表示手段
4511
データ暗号化鍵復号化手段
4505
情報記憶手段
4512
送信データ暗号化手段
4504
情報送受信手段
4540
4520
4521
中央制御手段
4524
情報送受信手段
4525
情報記憶手段
4530
4529
ICカード駆動手段
ICカード
4534
利用者情報管理手段
4531
受信データ復号化手段
4535
DVD情報管理手段
4532
送信データ暗号化手段
4536
現在時刻発生手段
4533
乱数発生手段
4537
使用有効期限判断手段

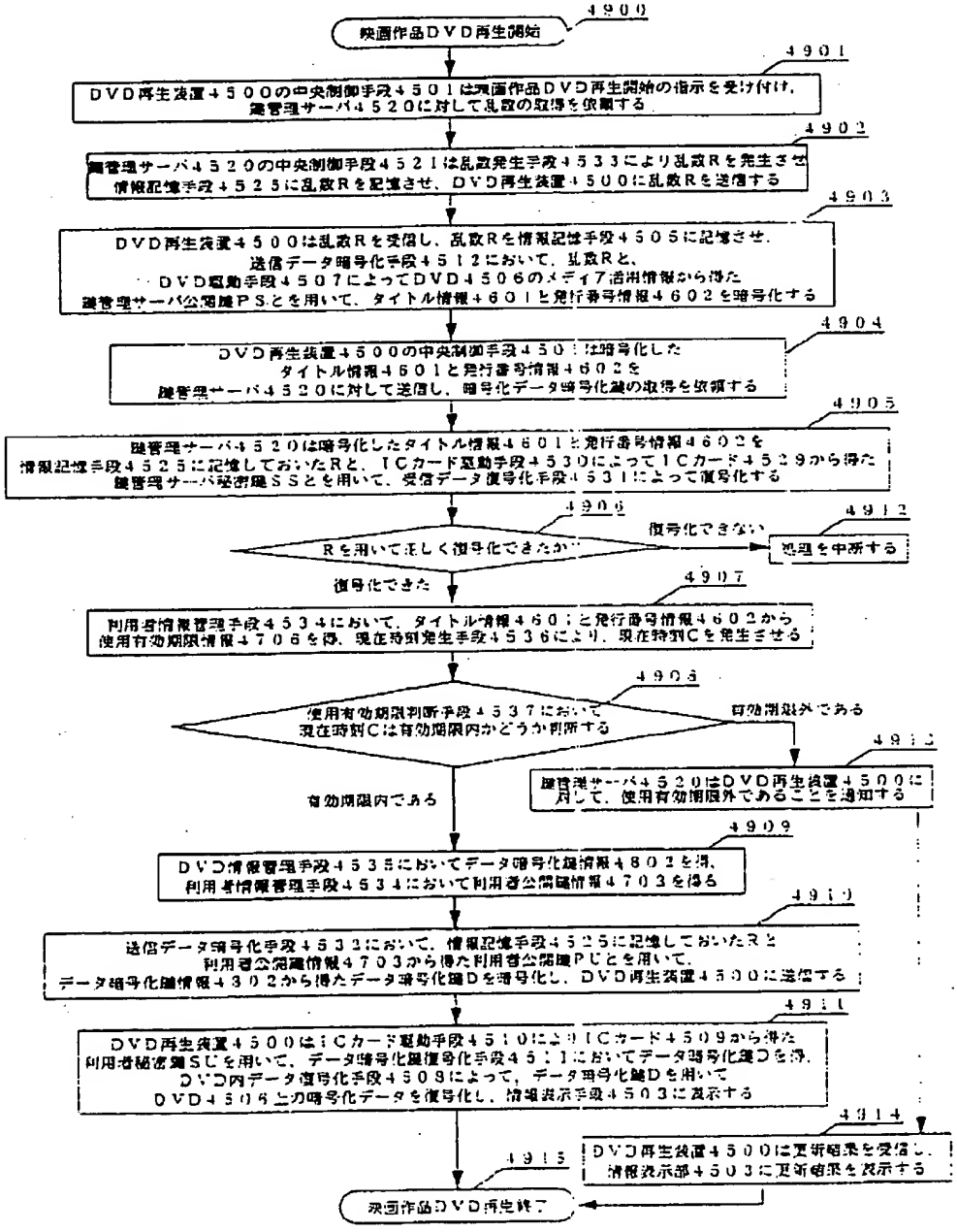
【図４７】


4700
利用者情報
4701
4702
4703
4706
タイトル情報
発行　号情報
利用者公開鍵情報
使用有効期限情報

【図４８】


４８００
DVD情報
４８０１
４８０２
タイトル情報
データ暗号化鍵情報

【図４９】


４９００
映画作品ＤＶＤ再生開始
４９０１
ＤＶＤ再生装置４５００の中央制御手段４５０１は映画作品ＤＶＤ再生開始の指示を受け付け、鍵管理サーバ４５２０に対して乱数の取得を依頼する
４９０２
鍵管理サーバ４５２０の中央制御手段４５２１は乱数発生手段４５３３により乱数Ｒを発生させ情報記憶手段４５２５に乱数Ｒを記憶させ、ＤＶＤ再生装置４５００に乱数Ｒを送信する
４９０３
ＤＶＤ再生装置４５００は乱数Ｒを受信し、乱数Ｒを情報記憶手段４５０５に記憶させ、送信データ暗号化手段４５１２において、乱数Ｒと、ＤＶＤ駆動手段４５０７によってＤＶＤ４５０６のメディア識別情報から得た鍵管理サーバ公開鍵ＰＳとを用いて、タイトル情報４６０１と発行番号情報４６０２を暗号化する
４９０４
ＤＶＤ再生装置４５００の中央制御手段４５０１は暗号化したタイトル情報４６０１と発行番号情報４６０２を鍵管理サーバ４５２０に対して送信し、暗号化データ暗号化鍵の取得を依頼する
４９０５
鍵管理サーバ４５２０は暗号化したタイトル情報４６０１と発行番号情報４６０２を情報記憶手段４５２５に記憶しておいたＲと、ＩＣカード駆動手段４５３０によってＩＣカード４５２９から得た鍵管理サーバ秘密鍵ＳＳとを用いて、受信データ復号化手段４５３１によって復号化する
４９０６
Ｒを用いて正しく復号化できたか
復号化できない
４９１２
処理を中断する
復号化できた
４９０７
利用者情報管理手段４５３４において、タイトル情報４６０１と発行番号情報４６０２から使用有効期限情報４７０６を得、現在時刻発生手段４５３６により、現在時刻Ｃを発生させる
４９０８
使用有効期限判断手段４５３７において現在時刻Ｃは有効期限内かどうか判断する
有効期限外である
４９１３
鍵管理サーバ４５２０はＤＶＤ再生装置４５００に対して、使用有効期限外であることを通知する
有効期限内である
４９０９
ＤＶＤ情報管理手段４５３５においてデータ暗号化鍵情報４８０２を得、利用者情報管理手段４５３４において利用者公開鍵情報４７０３を得る
４９１０
送信データ暗号化手段４５３２において、情報記憶手段４５２５に記憶しておいたＲと利用者公開鍵情報４７０３から得た利用者公開鍵ＰＵとを用いて、データ暗号化鍵情報４３０２から得たデータ暗号化鍵Ｄを暗号化し、ＤＶＤ再生装置４５００に送信する
４９１１
ＤＶＤ再生装置４５００はＩＣカード駆動手段４５１０によりＩＣカード４５０９から得た利用者秘密鍵ＳＵを用いて、データ暗号化鍵復号化手段４５１１においてデータ暗号化鍵Ｄを得、ＤＶＤ内データ復号化手段４５０８によって、データ暗号化鍵Ｄを用いてＤＶＤ４５０６上の暗号化データを復号化し、情報表示手段４５０３に表示する
４９１４
ＤＶＤ再生装置４５００は更新結果を受信し、情報表示部４５０３に更新結果を表示する
４９１５
映画作品ＤＶＤ再生終了

フロントページの続き

(51) Int. Cl.[6]	識別記号	FI	
		H04L 9/00	641